Approved on 1 July 2008 and lastly updated on 16 March 2018

Organisational, Management and Control Model of SNAITECH S.p.A. pursuant to art- 6, par. 3 of D.Lgs. n. 231/2001

TABLE OF CONTENT

GLOSSARY OF TERMS

"**Sensitive Activities**":	Companies activities which, by their nature, are potentially subject to one or more offences identified by the D.Lgs. no. 231/01
"CCNL":	National Collective Bargaining Agreement currently applied by SNAITECH S.p.A.
"**Ethical Code**":	Code of conducts containing crucial principles for SNAITECH S.p.A. as well as conducts and behaviours, which should inspire employees, of any grade, and directors when performing their duties
"**Corporate Controls**":	The system of proxies, procedures and internal controls aimed at ensuring a suitable transparency and knowledge of decision-making processes as well as conducts of senior managers and employees pursuant to art. 5 D.Lgs. no. 231/2001
"**Recipients**":	Corporate governance bodies, Independent Auditor, personnel - senior managers and employees – and third parties (including but not limited to: distribution network, advisors, suppliers of goods and services as well as any other party working for or on behalf on the Company)
"**Legislative Decree no. 231/01**" o "**Decree**":	Legislative Decree 8 June 2001, n0. 231 and any subsequent amendments and additions

"Individual in charge of a public service":	The title is assigned by exclusion, as it goes to those performing public interest activities, not consisting of simple or merely material tasks, governed in the same manner as public function, but which do not entail the powers typically assigned to a Public Official pursuant to art. 358 c.p.
"**Confindustria guidelines"**:	Guidelines (approved by Confindustria on 7 March 2002 and subsequently updated on 31 March 2008 and 31 March 2014) to implement and set up Organisational, Management and Control Models pursuant to D.Lgs. n. 231/2001.
"Model":	Organisational, Management and Control Model ruled by D.Lgs. n. 231/2001 or else the current document, including Special Sections (A, B, C, D, E, F, G, H, I, L, M, N O e P) and any other related annexes.
"Corporate Governance bodies":	Board of Directors, Statutory Auditors and any other body or individual attributed with powers of representation, decision and/or control of the Company
"**Supervisory Body**" o "**SB**":	Entity appointed pursuant to art. 6 of D.Lgs. no. 231/01 in charge of surveillance on the effectiveness and suitability of the Model, compliance with soundness and functioning requirements and required updates
"P.A.":	Public Administration and in relation to the offences against public administration, public officers and individuals in charge of public services.
"Public Official":	Individual holding a legislative, judiciary or administrative public office (art. 357 c.p.).
"Related Offences":	Offences identified by the Decree with related administrative liabilities as well as specific administrative offences ruled by the Decree

"**Company**" or "**SNAITECH**":	SNAITECH S.p.A. is a limited liability company listed on Milan stock exchange and acts as concessioner for all the activities pertaining to the offering and collection of horserace and sports bets on retail distribution network regularly performed under license issued by Agenzia delle Dogane e dei Monopoli ("ADM") (formerly Amministrazione Autonoma dei Monopoli di Stato). It acts as concessioner for the management of the AWPs electronic network (art. 110, par. 6, letter a) of TULPS) as well as VLTs electronic network (art. 110, par. 6, letter b) of TULPS) and any related activities duly performed under license C.I.G. 4607780C55 released by ADM. Furthermore and pursuant to Law n. 88 of 7 July 2009 ("EU Law"), SNAITECH was awarded with the license no. 15215 ("Online Gambling Concession") to offer online gambling in accordance with art. 24, par. 13, letter a) of the EU Law, which sets specific rules and conducts.
"**Disciplinary System**":	Disciplinary system and related sanctioning mechanisms for breaches of the Model
"**Senior Managers**":	Pursuant to art. 5 of D.Lgs. no. 231/01, any individual empowered with representation and management functions of the whole company or a division, with financial and functional autonomy, as well as any individual with powers, also de facto, of representation, decision and/or control of the Company
"**Employed reporting to Senior Managers**":	Pursuant to art. 5 of D.Lgs. no. 231/01, any employee reporting to head of division or under the supervision of Senior Managers.
"**Third parties**":	Any subject, individual or company, engaging with the Company (including but not limited to: distribution network, advisors, suppliers of goods and services as well as any other party working for or on behalf on the Company)

***Whistleblowing*:**

Any reporting of wrongdoing made by an employee or partner. Recipients of the whistleblowing regulation on private sector pursuant to Law 179/2017 are companies, groups, non-government organizations, no-profit entities, foundations and any other association implementing an Organisational, Management and Control Model pursuant to D.Lgs. 231/2001.

Document layout

The current document is composed by a General Section, an Introduction to Special Sections and 14 Special Sections.

The General Section reports main functions and principles of the Model as well as identifies and rules the key elements of the Model including Supervisory Body, set up and disclosure of the Model, Disciplinary System and the assessment and management of risks of offences.

The Introduction to Special Sections lists all the general prevention protocols applicable to transactions carried with sensitive areas.

Furthermore, the current document includes the following Special Sections as well as any additional annex which the document refers to:

- ***Special Section A**:*
  - ✓ Part 1: description of offences against the Public Administration (art. 24 e 25 of D.Lgs. no. 231/01);
  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to offences against the Public Administration, specific prevention protocols, reporting to SB and disciplinary sanctions.
- ***Special Section B**:*
  - ✓ Part 1: description of corporate offences (arti. 25-*ter* of D.Lgs. no. 231/01);
  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to corporate offences, specific prevention protocols, reporting to SB and disciplinary sanctions.
- ***Special Section C**:*
  - ✓ Part 1: description of crimes related to Market Abuse (art. 25-*sexies* of D.Lgs. no. 231/01);
  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to Market Abuse crimes, specific prevention protocols, reporting to SB and disciplinary sanctions.
- ***Special Section D**:*
  - ✓ Part 1: description of offences related to Occupational Safety and Health (art. 25-*septies of* D.Lgs. no.231/01);
  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to offences linked to Health and Occupational Safety, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section E**:*

  - ✓ Part 1: description of offences related to Handling stolen goods, laundering and use of money, assets or benefits whose origin is illegal (art. 25-*octies* of D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to Money Laundering offences, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section F**:*

  - ✓ Part 1: description of Computer crimes (art. 24-*bis* of D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to Computer crimes, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section G**:*

  - ✓ Part 1: description of offences related to Organised Crime (art. 24-*ter* of D.Lgs. no. 231/01) and Transnational Crimes (L. no. 146/2006);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to Organised Crime and Transnational Crimes, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section H**:*

  - ✓ Part 1: description of crimes against Industry and Trade (art. 25–*bis* of D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to crimes against Industry and Trade, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section I**:*

  - ✓ Part 1: description of offences related to Copyright Infringement (art. 25-*novies* of D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to Copyright Infringement, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section L**:*

  - ✓ Part 1: description of crimes related to Counterfeiting of money (art. 25-*bis of* D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to crimes connected to Counterfeiting of money, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section M***:

  - ✓ Part 1: description of offences related to the Omission or False or Misleading Statement to Judicial Authority (art. 25-*decies* of D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to offences in connection with the Omission or False or Misleading Statement to Judicial Authority, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section N***:

  - ✓ Part 1: description of Environmental crimes (art. 25-*undecies* of D.Lgs. no. 231/01);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to Environmental crimes, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section O***:

  - ✓ Part 1: description of offence related to Employment of Migrants with Invalid Residence Permits (art. 25-*duodecies* of D.Lgs. no. 231/2001);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to offence connected to the Employment of Migrants with Invalid Residence Permits, specific prevention protocols, reporting to SB and disciplinary sanctions.

- ***Special Section P***:

  - ✓ Part 1: description of crimes connected to Terrorism or subversion of the Democratic Order pursuant to criminal law and special regulations (art. 25-*quater* of D.Lgs. no. 231/2001);

  - ✓ Part 2: identification of areas and divisions where offences may be committed, potential sensitive activities related to crimes connected to Terrorism or subversion of the Democratic Order, specific prevention protocols, reporting to SB and disciplinary sanctions.

Notwithstanding the provisions of Special Sections A to P of the current document, SNAITECH set a specific system of proxies, procedures, protocols and internal controls to ensure full transparency and awareness of financial and decision-making processes as well as conduct and behaviour of each recipient of the Model.

The Disciplinary System and related sanctioning mechanism, to be applied in case of breach of the Model, is part of the current Model.

The Board of Directors has furthermore approved the Ethical Code, which forms a separate and different tool compared to the Model.

The Ethical Code reports key principles inspiring SNAITECH S.p.A. as well as disclosing conducts and behaviours held by any employee, of any grade, and directors when performing their corporate duties.

1. Legislative Decree no. 231 of 8 June 2001

1.1. Characteristics and natures of corporate liabilities

The Legislative Decree no. 231 of 8 June 2001 acknowledged the international regulation on bribery and introduced administrative liability regime applying to entities.

This kind of corporate liability combines both sides of the criminal and administrative sanction systems. According to the Decree, the entity is imposed with an administrative sanction, given the administrative nature of the offence, although the sanctions system relies on the criminal process: the public prosecutor is the relevant authority prosecuting crimes and the criminal court issues sanctions.

The entity's liability is additional to that of the natural person who was the perpetrator of the offence, and is independent of it, as it also exists where the perpetrator has not been identified or cannot be charged or where the offence is extinguished for a reason other than amnesty.

The entity may discharge its liabilities if implements effectively organisational and management models able to prevent offences and mitigate any involvement.

The entity may also benefits of several advantages if implements effectively the Model after the offences are challenged. In particular, if the offence is challenged before the first-degree hearing, the entity may benefit of: i) reduction of monetary penalties; ii) non application of interdictions and conversion into monetary penalties. If the offence is challenged after the hearing, the entity may benefit only of the conversion into monetary penalties.

If the entity does not implement the Model, it is deemed to be liable pursuant to art. 5 of D.Lgs. no. 231/2001. The only exclusion applies when the senior manager, who perpetrated the offence, acted only in his or her own self-interest or third-party interest: the entity is not considered liable in this circumstance.

The Decree applies to "legal persons, companies and associations, including those without legal personality", public economic authorities and concessioners. State, local authorities, non-economic public authorities and other entities of constitutional level (including political parties and unions) are out of scope.

1.2. List of crimes identified by the Decree and subsequent amendments

The entity is responsible only of those administrative crimes – Relative Offences – listed by the Decree or set by a specific law in force before the crimes were committed.

To date, the list of offences include the following:

i) Crimes against the Public Administration (art. 24 e 25);

ii) Computer Crimes (art. 24-*bis*);

iii) Offences related to Organised Crime (art. 24-*ter*)*;*

iv) Crimes related to Counterfeiting of money (art. 25-*bis*);

v) Crimes against Industry and Trade (art. 25-*bis*.1);

vi) Corporate offences (art. 25-*ter*) including bribery between individuals;

vii) Crimes connected to Terrorism or subversion of the Democratic Order (art. 25-*quater*);

viii) Practices involving female genital mutilation (art. 25-*quater*.1);

ix) Crimes against individual's character (art. 25-*quinquies*);

x) Market abuse (art. 25-*sexies*) e and related administrative offences;

xi) Culpable homicide and serious or life-threatening injury resulting from any violation of Health and Occupational Safety regulations (art. 25-*septies*);

xii) Handling stolen goods, laundering and use of money, assets or benefits whose origin is illegal (art. 25-*octies*);

xiii) Offences related to Copyright Infringement (art. 25-*novies*);

xiv) Offences related to the Omission or False or Misleading Statement to Judicial Authority (art. 25-*decies*);

xv) Environmental crimes (art. 25-*undecies*)*;*

xvi) Offences related to Employment of Migrants with Invalid Residence Permits (art. 25-*duodecies*);

xvii) Racism and xenophobia crimes (art. 25-*terdecies*)*;*

xviii) Liabilities from administrative offences pursuant to art. 12. of Law no. 9/2013;

xix) Transnational Crimes set forth by art. 10, Law no. 146 of 16 March 2006.

The application and importance of each offence are described on par. 2.12 of the current General Section.

1.3. Criteria for attribution of responsibilities to the entity

If a Relevant Offence (listed on par. 1.2) is committed, the entity is deemed responsible when certain conditions apply. These conditions set the relevant criteria to determine attribution of offences and may be divided into **objective** and **subjective** conditions.

The **first objective condition** requires the Relevant Offence to be committed by individuals having formal and qualified relationships with the entity. Art. 5 of the Decree identifies the following perpetrators:

- ***Individuals holding representative, administrative or management role in the entity or one of its division with financial and functional autonomy*** (Senior Managers) including legal representative, executive officer, head of division and any other individual managing the entity, also de facto. All these individuals have full power to make decision on behalf of the entity. Furthermore, the list includes any subject delegated by directors to manage, also de facto, the entity or one of the branches;

- ***Employees reporting to Senior Managers***. Employees and any other individual performing duties under direct reporting and supervision of Senior Managers. Advisors are also included in the list. Finally, the list includes also any external subject acting and performing duties on behalf of the entity, under specific working agreements and mandates.

The **second objective condition** requires the offence to be committed by the aforementioned subjects in the interest or to the advantage of the entity (art. 5, par. 1 of Decree).

- There is "***interest***" when the perpetrator acted to do favours for the entity, regardless the effective achievement;

- There is "***advantage***" when the entity benefited, or could have benefited (also non economic benefits) by the offence.

As specifically set forth by the law, the entity is not liable if Senior Managers or Employees reporting to Senior Managers acted in their own self-interest or third-party interest (art. 5, par. 2 of the Decree).

Subjective criteria set those conditions needed to attribute offences to the entity: exemption from liabilities is allowed where the entity can prove to have done everything to arrange, manage and prevent Related Offences listed in the Decree during the course of business. On this purpose, the Decree provides that an entity shall not be liable where it can prove, before the offence was committed, that:

- Adopted and implemented appropriate organisational and management models to prevent offences;
- It has established an internal control body (Supervisory Body) in charge of supervising the concrete functioning of the Model;
- There was no omission or insufficient control from the Supervisory Body.

For the entity to be exempted from liabilities, all the above conditions shall be satisfied simultaneously.

There is a presumption of guilt where offences are committed by Senior Managers, given they hold a representative, administrative or management role in the entity: exemption is allowed only if the entity may prove that the offence was committed by fraudulently circumventing the current Model and the SB conducted insufficient controls on the correct functioning and compliance with

the Model (art. 6 of Decree) [1]. In such circumstances, the Decree requires the entity to proof the unfamiliarity with the offences by demonstrating frauds perpetrated by Senior Mangers.

When Employees reporting to Senior Mangers commit the offence, the entity shall be liable if there was no compliance with management and supervision duties: exemption of liabilities is subordinated to the adoption of proper conduct protocols (set up in line with the type of organisation and business), which ensure compliance of activities with law as well as identify and promptly remove any potential risk (art. 7, par. 1 of Decree)[2]. It is therefore considered a real "fault of the organisation", because the entity indirectly allowed perpetration of offences by improperly controlling those activities and individuals potentially exposed to risk of Relevant Offences.

1.4. Guidelines provided by the Decree on characteristics of the organisational, management and control model

The Decree rules some general principles of the organisational, management and control model without providing any specific details. The model allows exemptions of liabilities if:

- It is effective or reasonably suitable to prevent offences;
- It is properly implemented or its content is embedded within internal corporate procedures and internal auditing system.

As regards the effectiveness of the Decree, the model shall have the following minimum provisions:

- Identify those activities, which may give rise to the offences listed in the Decree;
- Define the procedures through which the entity makes and implements decisions relating to the offences to be prevented;
- Define procedures for managing financial resources to prevent offences from being committed;
- Define specific protocols to plan training on prevention of crimes;

---

[1] *Pursuant art. 6, par. 1 of D.Lgs. no.231/01, "if the offence is committed by those individual listed in art. 5, par. 1, letter a) [Senior Managers], the entity shall not be liable if it may prove that: a) before the offence was committed, management adopted and effectively implemented organisational and management models aimed at preventing offences; b) the duties to supervise on functioning and compliance with models as well as ensuring constant update are attributed to an internal body with decision-making and control powers; c) individuals perpetrated the offence by fraudulently circumventing the models; d) there was no omission or insufficient controls by the internal body identified in letter b)."*

[2] Pursuant to art. 7, par. 1 of D.Lgs. no. 231/01, "*in accordance with art. 5, par. 1, letter b) [Employees reporting to Senior Managers], the entity is deemed liable if the offence was perpetrated because of the non compliance with management and control duties".*

- Put in place an effective disciplinary system to punish non-compliance with the measures required by the Model.

- Define specific training duties for the Supervisory Body;

- Adopt proper conduct protocols (set up in line with the type of organisation and business), which ensure compliance of activities with law as well as identify and promptly remove any potential risk.

The Decree requires the model to be subject to periodic control and update, either in the event of a breach or in the event of relevant changes of the entity's organisation or business or if changes of relevant regulations occurred, especially following the inclusion of new Relevant Offences.

1.5. Offences committed abroad

Pursuant to art. 4 of Decree[3], the entity may be liable for crimes committed abroad.

However, such circumstance is subordinated to the following conditions, set in additional to the aforementioned ones:

- Pursuant to art. 7[4], 8[5], 9[6] e 10[7] of C.P., there exist general conditions to prosecute in Italy a

---

3 Art. 4 of D.Lgs. no. 231/2001, "*Crimes committed abroad"* states *"in the events ruled by art. 7, 8, 9 and 10 of Criminal Law, entities with head office in Italy are liable of any crime committed abroad as long as the foreign country is has not started any proceeding. In those circumstances where the offender is punished upon request of the Minister of Justice, the entity is punished only if the request includes the entity as well"*.

4 Art. 7 of C.P., "*Crimes committed abroad*" states "*a citizen or a foreign individual committing crimes abroad is persecuted by the Italian law, if one of the following crime is committed: 1. Crimes against the State; 2. Crimes related to counterfeit the State seal and any possible use; 3. Crimes related to Counterfeiting of money and other Italian valuables; 4. Crimes committed by public officials by abusing of powers or breaching their duties; 5. Any other crime, recognised by special laws or international agreements, shall be subject to Italian Criminal Law"*.

5 Art. 8 of C.P., "*Political crimes committed abroad*" states: a *citizen or a foreign individual, who commits abroad a political crimes not included in point 1 of the previous article, is punished by the Italian law upon request of the Minister of Justice. If the crime is punishable upon complaint of the offended party, the complaint is needed in addition to the Minister's request. Political crime is defined by criminal law as any crime against a political interest of the State or a political right of a citizen. It is furthermore considered political crime any offence perpetrated, in part of or in full, by political reasons"*.

6 Art. 9 of C.P., "*Common crimes committed abroad by citizens*" states "*when a citizen commits abroad a crime (not included in the previous articles), which is punished by the Italian law with life sentence or at least 3 year prison sentence, the citizen shall be punished by the same law. If the crime is punishable with a shorter life sentence, the offender is punished upon request of the Minister of Justice or upon compliant of the offended party. In the events specified in previous articles, when crime is against the European community, a foreign state or citizen, the offender is punished upon request of the Minister of Justice as long as extradition was not allowed or accepted by the foreign state"*.

7 Art. 10 of C.P. "*Common crimes committed abroad by foreigners*" states: "*when a citizen commits abroad a crime against the State or a citizen (crimes not included in the articles 7 and 8), which is punished by the Italian law with life sentence or at least one year prison sentence, the citizen shall be punished upon request of the Minister of Justice or upon compliant of the offended party. When crime is against the European community, a foreign state or citizen, the offender is punished upon request of the Minister of Justice as long as: 1. Offender is within the Italian*

crime committed abroad;

- Entity has its head office in Italy;
- The offence is committed abroad by an individual formally connected with the entity;
- The country where the offence was committed does not initiate any proceeding.

1.6. Sanctions

In relation to administrative offences, the D.Lgs. no. 231/01 sets forth the following sanctions:

- ***Administrative fines and monetary sanctions;***
- ***Interdictions;***
- ***Confiscations;***
- ***Publication of the sentence.***

Administrative fine and monetary sanction is always imposed by the court when the entity is deemed liable. It is ruled by art. 10 and subsequent articles of the Decree and represents the basic sanction applicable to the entity.

The Regulator adopted a new criterion for the court to assess and attribute sanctions by imposing two different and subsequent steps. This allows the sanction to be more in line with the severity of the offence and the economic and financial health of the entity.

In the first step, the court shall quantify the number of shares (between 100 and 1,000) by taking into account:

- Severity of the offence;
- Degree of liability of the entity;
- Any activity implemented to remove or mitigate consequences of the offence and to prevent reiteration of any further offence.

In the second step, the court shall determine the value of each share within the possible range (between Euro 258.00 and Euro 1,459.00). Such amount is determined "*in accordance with the economic and financial health of the entity in order to ensure effectiveness of the fine*" (Art. 10 and 11, par. 2 of D.Lgs. no. 231/01).

---

territory; 2. It is a crime punished with life sentence or at least 3 year prison sentence; 3. Extradition was not allowed or accepted by the foreign state".

Art. 12 of D. Lgs. no. 231/01[8] provides with a list possible situations where reduction of sanctions may apply.

Interdiction measures set forth by Decree apply, along with administrative and monetary fines, only to those offences specifically ruled and sanctioned with:

- Prohibition on conducting business activities;
- Suspension or revocation of licenses and concessions;
- Prohibition on contracting with the public administration;
- Denial or revocation of funding and contributions;
- Prohibition on advertising products and services.

Furthermore, one of the two following conditions set forth by art. 13 of D.Lgs. no. 231/01 shall apply before attributing any interdiction measure:

- "*The entity had a relevant profit and the offence was perpetrated by Senior Mangers or Employees reporting to Senior Mangers if, in the latter circumstance, the offence was committed in a context of relevant organisational deficiencies"* or
- "*when the offence is reiterated*"[9].

Interdiction measures shall not apply when the offence is committed in the exclusive interest of the offender or third parties and the entity had minimum benefit if none or the pecuniary damage is irrelevant.

Such measures are usually temporary, between three months and two years, and on an exceptional basis may be permanent. They usually refer to the specific activities performed by the entity. They may be even applied on a precautionary basis, before the conviction, upon request of the public prosecutor when there are serious clues of liabilities of the entity and there is a material risk of further perpetration of the offence.

---

[8] Art. 12 of D.Lgs. no. 231/2001 "*Scenarios for reduction of sanctions*" states: "*1. Monetary sanction is halved and may not be set above Euro 103,291.00 when: a) the offender acted in its own or third-party interest and the entity had minimum benefit if none; b) The entity of monetary damage is irrelevant. 2. Monetary sanction is reduced to one third when, ahead of the first-degree hearing: a) the entity has fully indemnified any damage and removed any negative consequences or acted with this intention; b) the entity adopted and implemented an organisational model aimed at preventing offences similar to the one committed. 3 When both conditions specified in previous paragraphs apply, the sanction is reduced from half to two thirds. 4 Under no circumstances the monetary sanction may be lower than 10,329.00"*.

[9] Pursuant art. 20 of D.Lgs. no. 231/01 "*there is reiteration when the entity has been previously punished for an offence at least once, and it repeats the offence within a period of five years from last conviction*".

The interdiction measures do not apply when the entity had put in place any remedy envisaged by art. 17 of D.Lgs. no. 231/01 and more specifically, when the following conditions apply:

- "*The entity has fully indemnified any damage and removed any negative consequences or acted with this intention*";
- *"The entity removed any organisational deficiency and adopted and implemented an organisational model aimed at preventing offences similar to the one committed";*
- "*The entity made available the profit or benefit achieved in order to be confiscated*".

The Regulator has furthermore specified how prohibition on conducting business activities is residual compared to other interdiction measures.

Pursuant to art. 19 of D. Lgs. no. 231/0, the conviction always includes the **confiscation** of the price (money or any other economic advantage given or promised in order to induce a third party to commit the offence) or the profit (immediate economic advantage) generated by the offence, excluding the portion due to the offended party and any third party's rights acting in good faith.

Publication of the sentence in one or more newspapers, in full or in part, may be imposed by the court, along with the publication in the municipal notice board (where the company has its registered office) when interdiction measures apply. The Chancellery of court is in charge of the publication at the expenses of the entity.

All the sanctions are of administrative nature although imposed by the criminal court. The penalty framework set by the Decree is extremely severe both in terms of amount of monetary fines and potential impact of interdiction measures, which may seriously limit the ordinary course of business.

The final conviction of the entity is included in the register of Administrative sanctions.

1.7. Transformation of the entity

The Decree rules the liabilities of the entity in case of transformation, merger, split and sale of the company.

The fundamental principle states the sole liability of the entity to fulfil, with its own assets, obligations arising from monetary fine. Neither shareholders nor associates are directly liable with their own assets, regardless the legal nature of the entity.

Monetary fines, in general, follow the same principles set forth by civil laws in relation to liabilities of entities going under a transformation process. Any interdiction measure is attributed to the entity holding the business units involved in the offence.

After the transformation, the entity shall be still liable of any offence committed before the transformation. The new entity is therefore subject to any sanctions applicable to the original entity.

In the event of a merger, including merger by incorporation, the new entity shall be liable for any offence committed by all entities involved in the merger. If the merger was executed before the end of the hearing, the court shall take into account only the economic and financial health of the original entity (no reference to the new entity).

In the event of a split-up, the entities involved in the split are jointly liable for any offence committed before the split and shall repay any monetary fines with their own assets as long as the relevant business unit involved in the offence was partially acquired by the entity; any interdiction measures are applied to the entity (or entities) holding the relevant business unit involved in the offence. If the merger was executed before the end of the hearing, the court shall take into account only the economic and financial health of the original entity (no reference to the new entity).

In the event of sale or transfer of the entity involved with the offence, the buyer is jointly liable with the seller for any monetary fine, which may be imposed for an amount up to the value of the purchased entity and as long as the fines were recorded in the ledger or the buyer was aware of. Any interdiction measures are applied only to the entities holding the relevant business unit involved in the offence.

2. SNAITECH S.p.A.: business and activities performed

SNAITECH S.p.A. is a limited liability company listed on Milan stock exchange and acts as concessioner for all the activities pertaining to the offering and collection of horserace and sports bets on retail distribution network regularly performed under license issued by Agenzia delle Dogane e dei Monopoli ("ADM") (formerly Amministrazione Autonoma dei Monopoli di Stato). It acts as concessioner for the management of the AWPs electronic network (art. 110, par. 6, letter a) of TULPS) as well as VLTs electronic network (art. 110, par. 6, letter b) of TULPS) and any related activities duly performed under license C.I.G. 4607780C55 released by ADM. Furthermore and pursuant to Law n. 88 of 7 July 2009 ("EU Law"), SNAITECH was awarded with the license no. 15215 ("Online Gambling Concession") to offer online gambling in accordance with art. 24, par. 13, letter a) of the EU Law, which sets specific rules and conducts.

The Company manages gaming machines and any other gambling-related devices as well as the lease and management of telecommunication and electronic networks needed to offer gambling products and services and, additionally, the company promotes and arranges any kind of event related to sports, races, tournaments, games and any other forms of entertainment. SNAITECH acts also as service provider to third-party concessioner-client, by offering only logistical and technological services needed to accept and collect bets.

SNAITECH owns and manages horseracing tracks in Milan and Montecatini Terme and related areas, including training tracks and horse stables. The Company is also a shareholder of the main Italian horseracing tracks.

The subsidiary Teleippica S.r.l. acts in the TV broadcast industry and provides all authorised Italian points of sales with UnireTV channels, where horse races are broadcasted both in Italy and abroad. Teleippica broadcasts also SnaiTV channels, where sports and other events are broadcasted. Radio Snai also provide real time communication.

2.1. Corporate governance of the Company

- **Board of Directors**

The Company is governed by the Board of Directors. The number of Directors is between five and fourteen, all appointed by the Shareholders' Meeting. Appointment has a specific term and members may be re-elected. Pursuant to art 14 to 21 of By-laws, the Board shall dispatch ordinary and extraordinary business and affairs of the Company.

The Model is part of the complex system of procedures and controls required by the Corporate Governance of the Company.

- **Shareholders' Meeting**

The general meeting is entitled to resolve, in ordinary and extraordinary session, on any topic set forth by law and by-laws.

Any resolution of the Shareholders' meeting, taken in compliance with applicable regulation and By-laws, is deemed legally binding for any absent or dissenting shareholder.

- **Independent auditor**

The Shareholders' meeting of SNAITECH appointed an independent auditor, registered in the Special Register, to audit accounting records and bookkeeping.

2.2. Attribution of powers

Three different types of powers may be identified within SNAITECH's organisation:

- Powers attributed by resolution of the Board of Directors and with specific notary proxy;
- Powers for specific actions;
- Internal authorisations.

Powers attributed by the Board of Directors and with specific notary proxy allow engaging business with third parties. As general SNAITECH's rule, only those individual with such formal powers may act on behalf of the Company.

Specific powers are usually related to certain actions well identified and with clear deadline; they are usually attributed, with special proxy, by those subjects empowered with relevant powers.

Service orders rule the procedures to assess need, release, change or withdrawal of the notary powers of attorney. Internal authorisations empower employees (of any degree) to run internal processes.

These internal authorisations are released by the relevant division and are periodically updated to reflect any organisational change of the Company. Internal authorisations are usually implemented to limit the use of notary power of attorney.

2.3. Internal Audit and Risk Management System

A complex system of rules, procedures and organizational functions designed to support sound and prudent management of the company in line with its goals, by identifying, assessing, managing and monitoring key risks.

Each individual of SNAITECH is part of the system and shall contribute to ensure its proper functioning in the course of its duties.

- **Audit and Risk Committee**

The ***Audit and Risk Committee*** shall perform analysis, advises and proposals needed to support the Board of Directors when assessing and taking decisions on the Internal Audit and Risk Management System as well as approving the financial statements.

- **Supervisor of the Internal Audit and Risk Management System**

The Supervisor's role includes the following:

a) Identify key corporate risks in line with specifics of the Company and report periodically to the Board of Directors;
b) Implement the guidelines set by the Board of Directors by arranging design, implementation and management of the Internal System and assessing constantly its suitability and effectiveness;
c) Instruct the Internal Audit Function to investigate on specific operational areas and compliance with internal rules and procedures. In this circumstances, the Chairman of the Board of Directors, the Chairman of the Audit and Risk Committee and the Chairman of the Board of Statutory Auditors shall be informed simultaneously.
d) Inform promptly the Audit and Risk Committee or the Board of Directors on specific issues raised for their actions.

- **Internal Audit Function**

The ***Function in charge of the Internal Audit*** performs controls, assessments and recommendations on the design and proper functioning of the Internal Audit and Risk Management System with the aim to preserve its efficiency and effectiveness. Reports directly to the Supervisor of the Internal Audit and Risk Management System and reports indirectly, through the Audit and Risk Committee, to the Board of Directors and the Board of Statutory Auditors.

- The ***Board of Statutory Auditors*** shall ensure***:***

✓ *Compliance with law and corporate by-laws:*

✓ *Compliance with principles of sound management;*

✓ *Suitability of the organizational, administrative and accounting framework of the Company and reliability of the accounting system to fairly represent any business transactions.*

The Board of Statutory Auditors is composed by three regular auditors and two substitute auditors.

- ***Risk Manager***

The Board of Directors appointed the Risk Manager with the following responsibilities:

a) Set guidelines and risk management policies in accordance with corporate strategies and goals;
b) Identify and describe key risk categories;
c) Perform risk assessment activities in order to analyse, assess, mitigate and monitor risks with the aim to prioritise risk mitigation policies and contain any residual risk at reasonable levels for the management;
d) Ensure reporting to management and Board of Directors;
e) Ensure proper communication with Board of Directors on constant risks monitoring.

- **Director in charge of the accounting report**

The Board of Directors appointed the ***Director in charge of accounting reports*** to take care of monitoring and implementation of the internal auditing system pursuant to Law n. 262/2005. This system aims to set guidelines for the Company, pursuant to art. 154-bis of D.Lgs. n. 58/1998 on the production and disclosure of financial statements.

- ***Internal Audit*** **function**

The Internal Audit function is responsible of the following:

a) Assess, periodically and in line with international standards, the suitability and proper functioning of the Internal Audit and Risk Management System (IARMS) of the Company and the Group and ensure full compliance with those internal rules (regulations, guidelines, procedures and operational procedures, proxies and power of attorney, etc.) related to the development of internal processes;

b) Arrange periodic IARMS assessment reports to be discussed with management;

c) Develop activities to support corporate governance bodies and related divisions. On this purpose, a Risk-based plan is developed and approved by the Board of Directors with the aim to forecast any audit and 231-supervision tasks as well as monitor the implementation of any mitigation actions ("Assurance task");

d) Support the Management on IARMS-related topics in order to favour effectiveness, efficiency and the integration of controls ("Internal advisory");

e) Ensure independent monitoring as required by internal models as well as manage investigations (following anonymous reporting too);

f) Support control bodies (Audit and Risk Committee, Statutory Auditors, Supervisory Body) to perform their duties.

All the activities are performed autonomously with fairness, expertise and professionalism and full access to any information needed.

- **Anti-money laundering supervisor**

The AML supervisor responsibilities include:

- ✓ Cooperate to set internal controls and procedures system aimed at preventing and counteracting money laundering from illegal activities and terrorist financing set forth by the D. Lgs. no. 231 of 21 November 2007;
- ✓ Assess reliability of the data-feed system for the central archive and, along with other corporate bodies responsible of information, develop a suitable training program to provide constant training to employees and assistants;
- ✓ Prepare information flows addressed to corporate bodies and management as well as cooperate with Supervisory Body to supervise compliance with proceedings on anti money laundering related to illegal activities and terrorist financing.

- **Internal and external controls**

The following principles inspire the overall system of internal and external controls:

- ✓ **Segregation of duties**: assignment of duties and relevant authorization shall be designed to separate authorization, execution and control functions and, in any case, shall avoid concentration on a single individual;
- ✓ **Formalization of power of attorney and authorization**: such power shall be in line with the duties assigned and shall be attributed by proxies, which clearly specify the scope and relevant responsibilities;
- ✓ **Adherence to conduct rules of the Ethical Code**: all corporate procedures shall adhere to the principles of the Ethical Code;
- ✓ **Formalization of control**: all the relevant internal process shall be traceable (with documents or electronic support) and require direct control;
- ✓ **Description of process**: internal processes are ruled by specific procedures setting timing, implementation actions, decision-making processes and anomalies indicators.

2.4. Management and coordination activities and inspiring principles

SNAITECH performs management and coordination activities through several tasks aimed at planning strategically, economically and financially the Group, in full compliance with the operational autonomy of subsidiaries.

To prevent any offence related to management and coordination activities, the Company acts with fairness by balancing all the interests involved and by adhering to the following principles:

- Recipients of the Models shall operate in compliance with laws, Models prescriptions and principles of the Ethical Code, in order to prevent any of the offences included in the Decree;
- General prevention protocols (as better disclosed on par. 2 Introduction to Special Section);
- Communication and diffusion principles: SNAITECH fosters communication and diffusion of the conduct principles aforementioned with the aim of levelling all activities.

2.5. Model and Group undertakings

Each subsidiary choses to implement its own organisational, management and control model as well as its own ethical code. It must be approved by the relevant board once all the risks and mitigants have been identified and assessed.

When designing its own model, each Group undertaking shall comply with principles of the current document as well as Guidelines and Ethical Code implemented by SNAITECH. The model may include additional contents to reflect nature, dimension, type of business and the specific framework of internal proxies and authorisations.

The model of each Group undertaking is communicated to SNAITECHs' Board of Directors, which informs subsequently the Supervisory Body.

SNAITECH fosters communication between group undertakings in relation to: the degree of implementation of the system, pursuant to D.Lgs no. 231/01; any breach of the Model and sanctions

applied as well as any update, following the introduction of new Relevant Offences. In particular, the Supervisory Body of SNAITECH ensures proper relationship and communication between group undertakings, in order to produce prompt and complete information required to perform supervision duties. Communication shall include, among other things, all the activities planned and executed; any initiative taken; any mitigants; any critical issues reported. Communication aims to inform and gather attention of those business segments at risk.

As an example, the Supervisory Body of SNAITECH, in full compliance with the autonomy and confidentiality of information of undertakings, imposes to send to each supervisory body of each undertaking: i) key assessments planned; ii) reports of the supervisory board to the board of directors of each undertaking; iii) annual planning of meetings between supervisory bodies.

Furthermore, any relevant amendment to the model of an undertaking shall be reported by the supervisory body of the undertaking to the Supervisory Body of SNAITECH.

The Company shall foster principles, organisational and control rules in compliance with the ones included in the current Model.

2.6. Purposes of the Model

The Company adopts the Model with the aim to fully comply with the Decree as well as improve and make more efficient the current internal audit and corporate governance system.

Key goal of the Model is to produce a structured framework of principles and control procedures aimed at preventing, where possible and feasible, the perpetration of offences included in the Decree. The Model will be at the core of the Company governance and shall foster the diffusion of a business culture inspired to fairness, transparency and legality. The Model has, furthermore, the following purposes:

- Spread a business culture focused on legality. The Company rejects any non-compliant conduct with law or internal rules and in particular with provisions of the Model;
- Spread a business culture and attitude devoted to control and risk management;
- Effectively and efficiently arrange business activities focusing on decision-making processes and their traceability and transparency, accountability of decision-makers, design of preliminary and ex-post control as well as handling internal and external information;
- Implement all the relevant measures to minimise in the shortest time possible any risk of perpetrating the offences;
- Dispense proper training (different by content and delivery on the basis of qualification of recipients, level of risk and power of representation of the Company) to employees, individuals acting on behalf of the Company or having relevant business relationship with the Company in relation to those activities at risk.

2.7. Sources of the Model: Confindustria Guidelines

The Model was prepared in accordance with the Guidelines set forth by Confindustria on 7 March 2002 and subsequently updated on 31 March 2014.

The key indications of the Guidelines focus on the following:

a) Identification of Sensitive Activities;

b) Creation of an audit system to minimise risks by introducing specific procedures. This framework is furthermore supported by the framework of organisational structures, activities and operational rules implemented by the management and aimed at achieving goals of a valid audit system.

The most relevant elements of the preliminary control proposed by Confindustria are:

- Ethical Code;
- Organisational System;
- Manual and IT procedures;
- Authorisations and powers of attorney;
- Control and management systems;
- Communication of personnel and related training.

The audit system shall also be conformed to the following principles:

- Verifiability, traceability and consistency of each transaction;
- Separation of duties (no concentration of activities on a single individual);
- Traceability of controls;
- Effective Disciplinary System to sanction non-compliance with the measures required by the Model.

2.8. Model and Ethical Code

The Company has implemented, following the resolution of the Board of Directors, the Ethical Code, which is a different tool by nature, functions and contents.

The Ethical Code includes key inspiring principles for SNAITECH S.p.A. as well as day-to-day conducts rules to be followed for employees, of any grade, and directors.

The Model relies on full compliance with the Ethical Code and they together set a system of internal rules aimed at fostering a corporate culture lead by integrity, fairness, transparency,

confidentiality, safety of individual integrity and human dignity as well as occupational health and safety and environmental care.

2.9. Methodology followed to set SNAITECH S.p.A.'s Model

SNAITECH's Model was conceived based on its business and affairs, its corporate structure as well as the nature and size of the organisation. The Model is always subject to update to reflect the evolution of the company and relevant industry.

As per the Decree, SNAITECH mapped all the Sensitive Activities by identifying and assessing any risk related to the offences listed by the law and internal audit system as well as preparing first draft of the Model and subsequent updates.

The design/update of the Model was developed based on the following steps:

a) Preliminary assessment of the company, conducted through several meetings with key executives, in order to analyse the organisation and the activities as well as to identify corporate process and their concrete implementation;

b) Identification of those areas and processes exposed to possible offences, following the preliminary assessment mentioned in letter a), and the potential actions required to commit offences;

c) Analysis (with the support of those individuals responsible of the Sensitive Activities) of key risk factors related to the offences of the Decree as well as the detection, analysis and assessment of the appropriateness of current controls;

d) Identification of the areas of improvements of the internal audit system and relevant implementation plan.

At the end of these steps, it was produced/updated the list of Sensitive Activities or Company's divisions or processes potentially related to offences set forth by the Decree and related to the business and activities performed by the Company.

SNAITECH has therefore analysed the relevant internal controls (by assessing the Organisational System, the Proxy and Authorities system, the Internal Audit and any other relevant procedure (*as is analysis*)) and subsequently identified the relevant areas of improvement, produced specific suggestions and implementation plans (*gap analysis*).

Additionally, those areas and divisions in charge of financial and monetary instruments were furthermore assessed against the possibility to commit offences linked to Sensitive Activities.

SNAITECH has also carefully reviewed the residual elements of the Model, along with the activities of risk assessment:

- Ethical Code;
- Disciplinary System;
- SB regulation;
- SB information flow.

Maintenance of the Model is conducted periodically by the Company.

2.10. Recipients of the Model

The Model is addressed to any individual engaging business with the Company and ultimately committed to comply with its provisions.

In particular, Recipients of the Model are the following:

i. Corporate Governance bodies (Board of Directors, Board of Statutory Auditors, Independent Auditors and any other individual entrusted, also de facto, with powers of representations, control and decision-making);

ii. Personnel (employees and any other kind of collaborators) of the Company;

iii. Third parties, including Distribution Network, advisors, representatives, suppliers of goods and services and any other third party acting on behalf of the Company.

- ***Corporate Governance bodies and Personnel***

Directors, Statutory Auditors, Independent Auditors and Personnel are all recipients of the Model and shall comply with its provisions.

To assess the liabilities of the entity, Senior Managers includes directors, statutory auditors, executives and any other employee (non-director) with executive powers. Employees reporting to Senior Managers are the remaining employees (non-directors).

- ***Third parties***

Third parties include any individual subject to the Model for the specific role and duties performed within the Company, for example reporting functionally to a Senior Manager, or working, directly or indirectly, with SNAITECH.

- Any party involved with SNAITECH by a non-employment agreement (advisors, collaborators, etc.);
- Collaborators;
- Any individual acting on behalf of the Company;
- Individual with specific role and duties related to occupational health and safety (for example Relevant Practitioners and any non-employed officer in charge of Prevention);
- Distribution Network (points of sales, corners, etc.);
- Suppliers and partners (if any).

Third parties shall also include any other individual engaged in the business with other Group undertakings as long as they work on behalf of SNAITECH in sensitive areas.

SNAITECH considers the latest version of the Model and the Ethical Code a valid tool to sensitize employees and any other individual involved in the Company's business to have and impose fair and transparent conducts, in line with values of the Company and ultimately aimed at preventing any offence.

When dealing with third parties, SNAITECH includes specific contractual obligations, which impose the full compliance with principles of the Model and set express termination clauses.

SNAITECH adopts voluntary the Model required by the Decree, with the aim to spread and consolidate a corporate culture devoted to transparency and integrity as well as to ensure fair business conduct and preserve its own image, reputation and shareholders' expectations.

2.11. Amendments and updates of the Model

SNAITECH adopts and periodically updates its own Model in order to constantly ensure full legality, fairness and transparency of its business and affairs. SNAITECH has furthermore created the Supervisory Body to supervise, in accordance with provisions of the Decree, on functioning and compliance with the Model.

The Model was approved on 1 July 2008 and subsequently updated on 16 March 2018 in accordance with art. 6, par. 1, lett. a) of the Decree.

The Board of Directors is responsible, as stated by the law, for the adoption and the effective implementation of the Model.

Therefore, the Board of Directors is empowered to approve any update of the Model (seen as an effective way to implement it) by resolution and in accordance with the provisions set forth by the Model.

Any update, integration or amendment is aimed at ensuring the suitability of the Model to prevent any offence listed by the D.Lgs. no. 231/01.

The Supervisory Body may promote any amendments of the Model following the occurrence of any event, which may require updating and/or amending the Model.

The Supervisory Body shall report promptly to the Chief Executive Officer only in those circumstances of concrete urgency. In this case, the Chief Executive Officer shall summon the Board of Directors to take any relevant resolution.

If any corporate procedure of the Model is proved to be ineffective in preventing offences, this procedure shall be amended upon proposal of the relevant functions, with the opinion of the Supervisory Body.

The Model shall be promptly amended or integrated by the Board of Statutory Auditors when:

- There are relevant changes to the regulatory and organisational framework or to the Company's business;
- There are breaches or avoidance of the Model's prescriptions and the latter are no longer considered effective to prevent offences;
- In any other circumstance deemed necessary or useful.

2.12. Relevant offences for SNAITECH S.p.A.

Following the analysis conducted by the Company ahead of the Model preparation and update, the following list of offences (included in the D.Lgs. no. 231/10) was drafted:

- Crimes against the Public Administration (art. 24 e 25);
- Computer Crimes (art. 24-bis);
- Offences related to Organised Crime (art. 24-ter);
- Crimes related to Counterfeiting of money (art. 25-bis);
- Crimes against Industry and Trade (art. 25-bis.1);
- Corporate offences (art. 25-ter) including bribery between individuals;
- Crimes connected to Terrorism or subversion of the Democratic Order (art. 25-quater);
- Market abuse (art. 25-sexies) e and related administrative offences;
- Culpable homicide and serious or life-threatening injury resulting from any violation of Health and Occupational Safety regulations (art. 25-septies);
- Handling stolen goods, laundering and use of money, assets or benefits whose origin is illegal (art. 25-octies);
- Offences related to Copyright Infringement (art. 25-novies);
- Offences related to the Omission or False or Misleading Statement to Judicial Authority (art. 25-decies);
- Environmental crimes (art. 25-undecies);
- Offences related to Employment of Migrants with Invalid Residence Permits (art. 25-duodecies);
- Transnational Crimes set forth by art. 10, Law no. 146 of 16 March 2006.

Remaining offences and associated risks to perpetrate them are deemed low or irrelevant owing to the main business of the Company, the social and economic environment and legal and economical relationships with third parties. On this purpose, the relevant risks were controlled through the principles and conduct rules of the Ethical Code, which imposes Recipients to comply with fundamental values of parity, fairness, transparency, respect of individual and legality. Additionally, also the procedural system represents a valid garrison.

The Company is committed to constantly assess the importance of any additional offence currently envisaged by the D.Lgs. no.231/01 or included subsequently.

The Special Sections of the Model envisage, for any Relevant Offence for SNAITECH, those areas at risk, which include the activities where offences might occur, possible actions leading to the offences and current internal controls.

2.13. Tolerable risk concept

When arranging the Model it is important to determine the concept of "tolerable" risk.

It is important to set an effective threshold to limit the quantity/quality of the prevention measures to avoid perpetration of crimes.

Indeed, without identifying a threshold of "tolerable" risk, the quantity/quality of preliminary controls is potentially infinite, with obvious negative consequences on the company operations.

In relation to the preliminary control of offences set forth by the Decree, the tolerance level should be unavoidable but fraudulent behaviours.

This is in line with the topic of "fraudulent circumventing" the Model and its related limitation of liability for the entity (art. 6, par. 1, lett. c) "*offenders fraudulent circumventing the organisational and management model*"), as provided by the recent update of Confindustria's guidelines.

With specific reference to the disciplinary system introduced by the Decree, the tolerance level is reflected by the implementation of an effective prevention system, which may not be eluded unless done on purpose or the offenders have fraudulently circumvented the Model and internal controls.

2.14. Management of financial resources

Pursuant to art. 6, lett. c) of D.Lgs. no. 231/01, the Model shall identify the procedures to manage financial resources without perpetration of any crime. On this purpose, the Company adopts specific protocols and/or procedures reflecting principles and conduct rules to be followed when managing financial resources.

2.15. IT and manual procedures

SNAITECH set numerous procedures, within its organisational framework, to rule company's activities.

In line with Confindustria' Guidelines, the Company implemented several IT and manual procedures identifying the rules for each process and relevant controls to ensure fairness, effectiveness and efficiency.

The procedures are distributed, published and made available to the stakeholders by by Human Resource division and are always readable on the intranet.

3. Supervisory Body

3.1. Function

As requested by the Decree, the Company constitutes an independent and autonomous Supervisory Body with power of controls on risks arising from the Company's business and affairs.

The Supervisory Body shall constantly supervise on the following:

- Compliance with the Model by the aforementioned Recipients;
- Effectiveness of the Model to prevent the offences ruled by the Decree;
- Implementation of indications and prescriptions of the Model when performing Company's activities;
- Update of the Model in the event of relevant changes to the entity's organisation, business or regulations.

The Supervisory Body shall produce and approved its own internal governing rules, which shall be disclosed to the Board of Directors.

3.2. Requirements and composition of the Supervisory Body

According to art. 6 and 7 of the D.Lgs. no. 231/01, the indications to D.Lgs. 231/01 and the academic and legal views on this topic, the Supervisory Body shall have the following characteristics to ensure effective and efficient implementation of the Model:

a) Autonomy and independency;

b) Professionalism;

c) Continuity;

d) Integrity.

Autonomy and independency

These two characteristics of the Supervisory Body, and its components, are key to ensure an effective control.

Both concepts shall be defined within the relevant operational framework. Its position within the entity's organisation shall ensure independency and autonomy from any other body of the entity and specifically from Senior Managers and corporate governance bodies, in order to ensure properly supervision. On this purpose, the Supervisory Body shall have the highest hierarchical level in the organisation and shall report to the Board of Directors only.

Furthermore, the Board of Directors attributes to the Supervisory Body specific resources, set in in line with its duties, and approves a budget and financial resources, upon request of the Supervisory Body, to properly perform its duties (need of specific advisory, business trips, etc.).

Autonomy and independency of each member shall be determined according to its role and duties. Therefore, a single member may not overlapping roles, including operational, decision-making and management, which may affect the whole SB. Under no circumstances, autonomy and independency are subordinated to the absence of any conflict of interest with the Company.

a) Professionalism

The SB shall have technical and professional skills in line with the roles and duties attributes. Professional requirements along with independency typically ensure objective valuations.

Members of the SB are therefore required to have legal, auditing and risk management expertise. The SB might also rely on external advisors with special expertise on the activities exposed to Relevant Offences. The SB shall have working knowledge of principles and techniques of compliance and internal audit.

b) Continuity

The SB shall:

- Perform continuously any supervisory activity with the right level of commitment and relevant powers of inspections;
- Be a reference within the Company, to ensure continuity of the supervisory activity;
- Safeguard implementation of the Model and any update;
- Refrain from performing any other operational activity, which may influence the SB vision.

c) Integrity

Members of the SB must fulfil the following requirements:

- Shall not be subject of any temporary interdiction or suspension from the role of directors performed in legal persons and corporations;
- Shall not fall into the ineligibility or disqualification conditions set forth by art. 2382 C.C. for Directors and applicable also to members of the SB;
- Shall not be subject to any prevention measures pursuant to Law no. 1423 of 27 December 1956 ("*Prevention measures against individual deemed dangerous for public safety and morality*") or Law no. 575 of 31 May 1965 ("Provisions against mafia") and subsequent amendments and additions. This excludes any rehabilitation procedure;
- Shall not be convicted, even if the sentence is conditionally suspended, excluding any rehabilitation process:
  - ✓ Offences included in the R.D. 16 March 1942, n. 267 (Bankruptcy law);

- ✓ Offences included in the Section XI, Book V of Civil Code ("*Criminal provisions related to companies and consortiums*");
- ✓ Non-culpable crime with prison sentence of at least one year;
- ✓ Offences against Public Administration, public faith, pubic heritage and public economy.

Members of SB must also fulfil the requirements set forth by the MEF Decree n. 1845/Strategue/UD of 28 June 2011, following art. 1, par. 78, letter a), point 5 of Law no. 220 of 13 December 2010 and subsequent amendments and additions.

Each member shall submit a declaration to fulfil all the requirements.

If any of the requirements is no longer applicable, the member of the SB is removed according to par. 3.3.

3.3. Eligibility requirements

Members of the SB must have proved experience in the areas of internal control, administration and finance.

The following reasons represent ineligibility or loss of SB membership status:

a) The Integrity requirements aforementioned are no longer applicable;

b) The member is related by marriage or within the fourth degree of consanguinity or affinity with any member of the Board of Directors, Statutory Auditors or Independent Auditor;

c) Being subject to interdiction measures pursuant to D. Lgs no. 159 of 6 September 2011 (<<Anti-Mafia laws and precautionary measures including new provisions pursuant to art. 1 and 2 of Law mo.136 of 13 August 2010>>);

d) A non-final sentence, equivalent to the sentence issued pursuant to art. 444 of the Code of Criminal Procedure, even if suspended, for one of the crimes set forth under Legislative Decree 231/01 or a non-culpable crime;

e) Being subject to interdiction, bankruptcy or convicted, also with a non-final sentence, to crimes which may cause interdiction, also temporary, from public offices or ineligibility to perform management duties;

f) Being subject to administrative sanctions pursuant to art. 187-quater of the D.Lgs. no. 58 of 24 February 1998;

g) Existence of any financial relationship between any external advisor of the SB and the Company, such that the independency of the SB may be compromised.

During the mandate, if any one of the above reasons applies, the member of the SB shall promptly inform the Board of Directors and refrain from taking any further decision or action. The SB shall run with reduced membership until the Board of Directors appoints a new member.

3.4. Appointment, revocation, replacement, renouncement and disqualification from office

The SB is appointed for the whole period set by the appointment act and may be renewed.

Termination of the SB may occur under the following circumstances:

- Expiry of the mandate;
- Just cause for withdrawal by the Board of Directors;
- Renouncement of a member by written communication to the Board of Directors;
- One of the ineligibility reasons applies.

Revocation of the SB may occur only for just cause when on the following scenario applies:

- A member is part of a criminal proceeding related to one of the offences under D.Lgs. no. 231/01, of which the Company may be liable for;
- Breach of confidentiality duties of the SB;
- Gross misconduct in performing their duties;
- Involvement of the Company in a civil or criminal proceeding related to an insufficient or omitted supervision (also culpable) by the SB;
- Attribution of powers, offices and responsibilities within the organisation deemed non-compatible with the requirements of autonomy, independency and continuity of the SB. Any organisational measure related to a member of the SB (eg. termination of the employment, change of duties, redundancy, disciplinary actions, appointment as manager) shall be reported to the Board of Directors by the chairman of the SB;
- Unauthorised absence to two or more subsequent meetings of the SB, following proper call;
- Have been convicted, even if the sentence has been conditionally suspended, for one of the offences under D.Lgs. no. 231/01;
- Impediment of the member of the SB for a period longer than six months, following the occurrence of one of the causes of impediment set forth in par. 3.5;

Revocation is ruled with a qualified resolution (two/third) of the Board of Directors with the non-binding option of the Statutory Auditors. Each member of the SB may renounce in accordance with the procedure set forth by the regulation of the SB.

In the event of expiry, revocation or renounce, the Board of Directors shall promptly appoint the new member. The leaving member shall remain until replacement.

3.5. Causes of temporary impediment

If a member of the SB is temporary prevented, for at least six months, to perform its duties or have an autonomous and independent conduct, he or she shall disclose its impediments and the causes, when related to a conflict of interest. The member shall not join meetings of the SB or any specific resolution, pertaining to the conflict of interest, until the impediment is removed.

In the event of a temporary impediment or any other circumstance, which prevent one or more members to join meetings, the SB shall run with a reduced membership.

3.6. Activities and powers

In compliance with the indications of the Decree and the Guidelines, the SB shall have the following functions:

- Supervising the effective implementation of the Model: oversee behaviours of Recipients in compliance with Model;
- Assessing the effectiveness and adequacy of the Model and its ability to prevent any of the offence included in the Decree;
- Updating of the Model to reflect any amendment related to possible changes in the organisational, regulation and corporate structure;
- Verifying the effective adoption and implementation of any update of the Model by the Board of Directors.

When performing its functions, the SB shall comply with the following duties:

- Periodically assess the adequacy of the Internal Controls performed in relation to Sensitive Activities. On this purpose, the Recipient of the Model shall report to the SB any event that may expose the Company to potential offences. Communication must be in writing and addressed to the specific email address of the SB;
- Run periodic assessments and inspections on specific transactions and actions related to Sensitive Activities, in line with actions plan of the SB;
- Collect, analyse and maintain any relevant information for the Model (included reporting as per par. 3.8) and update the list of information to be received by the SB;
- Run internal investigations to assess any potential offence (related to the Model) recorded during supervision activities or specifically reported to the SB;
- Verify the effective adoption and implementation of the Internal Controls envisaged in the Model, in compliance with D.Lgs. no. 231/01 and intervene, where necessary, to update or amend any action;
- Promote, through relevant bodies and functions, any suitable initiative aimed at increasing awareness and understanding of the Model.

In order to perform the aforementioned functions and duties, the SB is entitled with the following powers:

- Have full access to any document and specifically to those ones related to contractual and non-contractual relationships between the Company and third parties;
- Rely on support and cooperation of corporate structures and governance bodies involved, or interested somehow, in the auditing activities;
- Arrange annual plans to assess suitability and functioning of the Model;
- Control the constant update of the Sensitive Activities list and propose any eventual amendments, in accordance with the principles and procedures required to update the Model;
- Attribute specific advisory and assistance tasks to external advisors. On this purpose, when appointing the SB, the Board of Directors approves a specific budget for the SB.

3.7. Information flows to and from the SB

Pursuant to art. 6, par. 2, point d) of the Decree, the Model must envisage specific information rights and duties for SB. They should relate to any offence committed against the Model, corporate procedures and Ethical Code.

The SB must be promptly informed by any individual and third party, subject to the Model, of any information related to possible offence.

The information duty is also extended to any corporate function and structure potentially exposed to the risk of perpetrating any Related Offences ruled by the Model.

3.7.1. Information flows to the SB

All the Recipients of the Model shall report any useful information to allow the SB assessing the effective implementation of the Model.

The information flow originates from the identification of those sensitive activities, which may be subject to the perpetration (direct or indirect, fraudulently or due to lack of control) of one of the offences under the D.Lgs. no. 231/01.

The Company, together with the SB, has implemented the procedure "Management of the information flows to the SB", which determines the type of information to be reported by those individuals involved in the sensitive activities, the frequency and procedures to be followed when reporting to the SB.

3.7.2. Information flows from the SB

The Board of Directors is responsible to adopt and effectively implement the Model. However, the SB shall report on the effective implementation of the Model and the occurrence of any critical aspect.

The SB must report:

- Promptly to the Chief Executive Officer on any specific and urgent issue related to sensitive activities;

- Periodically to the Board of Directors and Statutory Auditors. In particular, the SB must:

  - ✓ Report, in the annual statement provided at the beginning of each period, the annual action plan to be executed;

  - ✓ Arrange two semi annual statements, of which the second one summarises the activities performed during the year and the activities to be carried out in the first semester of next year.

The Management, the Chairman, the Chief Executive Officer and the Statutory Auditors may summon the SB at any time. Similarly, the SB may interact with the above-mentioned bodies to report on specific situations or on the functioning of the Model.

Any meeting with the SB shall be recorded. A copy of each record shall be kept by the SB and the relevant bodies involved from time to time.

Furthermore, under specific circumstances, the SB may:

(a) Report any assessment results to individuals in charge of functions and processes when there are potential areas of improvements. The SB, together with those individuals in charge, shall agree on the action plan, timing and results of the implementation.

(b) Report to the Board of Directors or the Statutory Auditors any conduct/action taken against the Model in order to:

  - Provide the Board of Directors with any relevant information needed to inform the relevant structures, assess and impose any disciplinary sanctions.

  - Provide instructions to remove any weakness and avoid any further perpetration of the offence.

The SB must promptly inform the Statutory Auditors if the offence is committed by the Board of Directors.

Finally, within SNAITECH Group, the SB of the Company shall liaise with the SB of the other undertakings.

3.8. Whistleblowing

Law no. 179 of 30 November 2017 "*Provisions to protect whistleblowers on public and private field*" introduced specific rules for those entities subject to D.Lgs. no. 231/01, with the aim to harmonise public law provisions with the new Law no. 179. Additionally, three more paragraphs (par. 2-bis, 2-ter and 2-quarter) were included on art. 6 of D.Lgs. no. 231/01.

In particular, art. 6 envisages on the following paragraphs:

- Par. 2-bis. The Organisational, Management and Control Models shall:

  - Have one or more information channels, which allow those individuals specified on art. 5, par. 1 letter a) and b)[10], to report any wrongdoing relevant for the Decree and based on specific elements or any breach of the model. These channels shall preserve the identity of whistleblower when handling reports.

  - Have at least one alternative channel, which preserve the identity of the whistleblower with IT procedures;

  - Prohibit any direct or indirect retaliation or discrimination of the whistleblower due to the his or her report;

  - Include, in the disciplinary system implemented in accordance with par. 2 letter e), sanctions to be imposed to those individuals breaching any confidentiality measures as well as acting with fraud or gross negligence when reporting groundless wrongdoings.

- Par. 2-ter. Any discrimination of the whistleblower, as identified on par. 2-bis, may be reported to the Labor Inspectorate by the whistleblower and the union selected by the whistleblower.

- Par. 2-quarter. Any retaliatory or discriminatory redundancy of the whistleblower shall be void as well as any change of duties pursuant to art. 2103 C.C. and any other retaliatory or discriminatory action taken against the whistleblower.

Furthermore, following a wrongdoing reporting, any litigations related to disciplinary actions and sanctions, demotion, redundancy, transfer and any other actions with negative impact, direct or indirect, on the employment relationship shall be justified by the employer as totally unrelated to the whistleblowing.

---

a) [10] Art. 5, par. 1 of D. Lgs. n. 231/2001 states: "*The entity is liable of any offence committed in its own interest or for its own benefit by individuals empowered with representation and management functions of the whole company or a division, with financial and functional autonomy, as well as any individual with powers, also de facto, of representation, decision and/or control of the Company*

b) *by individuals reporting to one of the subject under letter a)*".

The Whistleblowing Law introduced in the Italian legal system a new set of rules aimed at improving the effectiveness of anti-bribery tools as well as increasing protection of whistleblowers by encouraging reporting of wrongdoing or breaches of organisational, management and control models. Following a wrongdoing reporting, any litigations related to disciplinary actions and sanctions, demotion, redundancy, transfer and any other actions with negative impact, direct or indirect, on the employment relationship shall be justified by the employer as totally unrelated to the whistleblowing (the burden of proof will be reverted in such cases).

3.8.1. Whistleblowing procedure

Since the first implementation of the Organisational, Management and Control Model until the Whistleblowing Law come into force, the Company put extreme emphasis on the issue of reporting and ruled the information flows, according to par. 3.7.1.

To implement additions of art. 6 of D.Lgs. no. 231/01, the Organisational, Management and Control Model shall include a procedure to report wrongdoing, which protect the identity of whistleblower and his or her confidentiality right. On this purpose, the disciplinary system shall include specific sanctions for any retaliation or discrimination of the whistleblower, who acted, with good faith and on relevant ground, to report any wrongdoing or violation of the Model or the Ethical Code.

To ensure effectiveness of whistleblowing, the Company implemented a procedure "report of wrongdoing" for its employees, management, directors and third parties. They should all be informed of the existence of specific channels, which allow reporting wrongdoing, based on relevant ground, and ensure confidentiality (also with IT procedures).

The Company furthermore provides specific information to employees and third parties on procedures, rules and risks as well as ensuring acknowledgment and understanding of goals and motivation behind any reporting.

3.8.1.1. Scope of work and reporting channels of whistleblowing procedure

The procedure adopted by the Company aims to rule, induce and protect any subject, who become aware of any wrongdoing or relevant breach (according to D.Lgs. 231/01), and decides to report it.

Reporting shall therefore includes:

- Wrongdoing related to one or more offences for which the entity may be liable, according to the Decree;
- Conducts, unrelated to any offence, which however may result in breach of conducts, procedures, protocols and provisions of the Model.

It shall not be taken into account any report related to personal affair, employment relationship or direct reporting with other colleagues of the whistleblower.

Reporting shall provide useful elements to assess and conduct proper investigations (art. 6, par. 2-bis, D.Lgs. no. 231/2001).

Anonymous reporting shall be ruled as well although no confidentiality right is given in this case (art. 6, par. 2-ter e 2-quater, D.Lgs. no. 231/2001). Furthermore, it will be considered if properly detailed and related to severe crimes only.

Recipients of wrongdoing for the Company are:

- Members of the Supervisory Body;
- The Committee (Head of Legal and General Affairs, Head of HR and Organisation, Head of Internal Audit and a member of the SB).

Any reporting shall be addressed to odvsnai@snaitech.it or by ordinary mail to the SB:

Organismo di Vigilanza

SNAITECH S.p.A.

Piazza della Repubblica n. 32

20124 - Milano

In compliance with the law, the Company set an additional information channel able to protect the identity of the whistleblower.

Therefore, the whistleblower may report also:

- Verbally to the aforementioned Recipients;
- Through specific software, available on the intranet, which ensures confidentiality of whistleblower and reporting (in compliance with law).

The Company and recipients shall act in order to prevent whistleblowers against any kind of retaliation or direct/indirect discrimination, directly or indirectly, related to the report.

The "reporting wrongdoing procedure" adopted by the Company shall list duties and activities carried out by recipients in order to assess ground of report.

To foster a culture of legality and utilisation of reporting system, the Company shall inform its employees on the reporting procedure.

4. Disciplinary System

4.1. General Principles

The Company acknowledges and recognises that the effectiveness of the Model is subordinated to the implementation of relevant Disciplinary System against any offence included in the Model and Internal Controls.

On this purpose, articles 6, par. 2, letter e) and 7, par. 4, letter b) of the Decree state that organisational and management Models shall "*contemplate a suitable disciplinary system to punish any possible breach of the provisions of the model*" by the Senior Managers and Employees reporting to Senior Manager. Pursuant to art. 2106 C.C., in relation to employment agreements, the current Disciplinary System is part of the National Collective Bargaining Agreements applicable to employees.

Pursuant to art. 2095 C.C., the Disciplinary System is divided into sections according to the grade of the recipients.

Any breach of conducts rules and provisions of the Model committed by employees and directors of the Company is considered as a failure to comply with the employment obligations, pursuant to articles 2104 and 2016 C.C.

The sanctions of the Disciplinary System are unrelated to the outcome of a criminal proceeding, since conduct rules of the Model and Internal controls are adopted by the Company regardless the potential offences set forth by the Decree.

Precisely, failure to comply with provisions of the Model and Internal Controls may prejudice the relationship with the Company and cause possible sanctions, regardless any eventual criminal proceeding. This shall comply with timeliness (also from a disciplinary point of view) of the dispute and sanction, in accordance with current laws.

To assess the effectiveness and suitability of the Model in preventing the offences included in the D.Lgs. no. 231/01, it is necessary that the Model identifies and punishes any conduct potentially leading to offences.

The Disciplinary System shall commensurate different applicable sanctions to the dangerousness of conducts in relation to possible offences.

The Disciplinary System is therefore conceived to punish any offence against the Model, from the softest one to the most severe, by introducing different grades of sanctions and, secondarily, by setting a proportion between offences and sanction.

Regardless the nature of the Disciplinary System required by D.Lgs. no. 231/01 and the national bargaining agreement, the employer has full power to rule, pursuant to art. 2106 C.C., all categories of employees.

4.2. Definition of "breach" under the current Disciplinary System

In general terms, a breach of the Model and Internal Controls is defined as follows:

a) Any wrongdoing against provisions of the Model and Internal Controls, which corresponds to one of the offences of the Decree;

b) Any action or omission against the provisions of the Model and Internal Controls, which may lead to one of the offences of the Decree;

c) Any omission of action and conduct required by the Model and Internal Controls, which may not lead to one of the offences of the Decree;

d) Any action or conduct non compliant with the Whistleblowing Law no. 179/2017 and any subsequent additions and amendments.

4.3. Criteria to impose sanctions

The kind and size of sanctions is commensurate to the severity of the breach and shall adhere to the following criteria:

- Subjective part of the conduct (fraud, negligence);
- Relevance of duties breached;
- Potential damage suffered by the Company and the eventual sanction set by the Decree;
- Grade and hierarchy level of the offender;
- Aggravating and mitigating circumstances in relation to previous duties performed by the Recipient of the Model and any previous disciplinary actions;
- Any joint liability with other employees and third parties involved in the offence.

In the event of one of more breaches and applicable sanctions, the most severe sanction only shall apply.

Principles of timeliness and promptness of the dispute require imposing any sanction (mainly disciplinary) regardless of any criminal judgement.

Under no circumstance, disciplinary sanctions shall be imposed according to art. 7 of Law no. 300/07 ("Employees statute") and any other relevant regulatory and contractual provisions.

4.4. Sanctions

4.4.1. Employees: disciplinary offences

Disciplinary offence refers to any conduct or behaviour of employees, and directors, against rules and principles of the Model. The kind and size of sanctions is commensurate to the severity of the breach and to the following criteria:

- Conduct (fraud or negligence);
- Duties and grade of employee;
- Importance of the duty breached;
- Potential damage to SNAITECH;
- Reiteration of the offence.

In the event of one of more breaches and applicable sanctions, the most severe sanction only shall apply. A breach may result in a failure to comply with employment obligations, pursuant to art. 2104, 2106 and 2118 C.C., Employees statute, Law no. 604/66 (as amended by Law. No. 92/2012), current CCNL and art. 2119 C.C. where applicable.

4.4.2. Commensurability criteria

In order to provide criteria of commensurability between offences and disciplinary actions, the Board of Directors identify possible actions of employees, directors and third parties as follows:

- Conducts envisaging non execution of orders given by SNAITECH, both written or verbal, to perform any activity potentially leading to offences, including for example: breach of procedures, rules, written instructions, minutes or Ethical Code that may lead to negligence (minor breach);
- Conducts envisaging a material breach of discipline and/or diligence when performing any of the activities aforementioned with fraud or gross negligence (severe breach);
- Conducts harmful (morally or materially) for the Company that require immediate interruption of the employment. These include conducts leading to one or more Related Offences set forth by the Decree (severe breach with prejudice for SNAITECH).

Specifically, the following breaches envisage non-compliance with the Model:

- Breaches related to Sensitive Activities listed in the summary of the Model (Special Sections A, B, C, D, E, F, G, H, I, L, M, N, O, P);
- Breaches eligible (for the subjective part of the conduct) for Relevant Offences under the Decree;
- Breaches aimed to perpetrate offences under the Decree, which the Company may be liable for.

Non-compliance with the confidentiality rights required by the Whistleblowing Law no. 179/2017 as well as any retaliation or discrimination of the whistleblower constitutes breach of the Model.

Offences related to Health and Occupational Safety (Special Section D) are also included and sorted by severity.

In particular, there is a breach of the Model when the misconduct produces:

- A real danger for the physical integrity of one or more individuals including the offender;
- An injury to the physical integrity of one or more individuals including the offender;
- A severe injury, pursuant to art. 582, par. 1 of Criminal Law, to the physical integrity of one or more individuals including the offender;
- An extremely severe injury to the physical integrity, pursuant to art. 583, par. 2 of Criminal Law;
- The death of one or more individuals, including the offender.

4.4.3. Sanctions for middle managers and employees

In accordance with the Employee' statute, the relevant CCNL and any other legal and regulatory provision, the employee, who is liable for actions or omissions against the Model and Whistleblowing law, shall be subject to the following disciplinary sanctions based on the severity of his or her conducts and any reiteration of the offence:

- Verbal warning (minor breaches);
- Written warning (minor breaches);
- Fine up to three hours of salary (severe breaches);
- Suspension from work without salary payment up to three days (severe breaches);
- Immediate redundancy (severe breaches with prejudice for SNAITECH).

4.4.4. Sanctions for managers

Despite the disciplinary proceeding ex art. 7 of Law 300/07 is not applicable to managers, it is deemed relevant to extend to managers the same procedures of the Employees' statute.

In case of any offence (including direct breach of the Model, the laws (including whistleblowing laws and principles), the rules and internal procedures of the Model) perpetrated by managers when performing tasks related to sensitive areas, the Company shall impose to the offenders the following sanctions, also taking into account the severity of the offence and any eventual reiteration.

Given the specific nature of the relationship, their duties to enforce compliance with Model, the provisions of the current laws and CCNL for managers, the Company shall dismiss with notice or just cause the manager in case of severe breaches.

Given the possibility to dismiss managers, the Company shall apply commensurable sanctions for minor offences including written warning or suspension from work without salary up to ten days.

The Company may still claim a compensation for any damage inflicted by the manager.

4.4.5. Measures against Directors, Statutory Auditors and Supervisory Body

- **Measures against Directors**

When the SB, Statutory Auditors and Board of Directors notice a breach of the Model by one or more Directors, they shall promptly inform the Board of Directors, which in turn shall take all the necessary actions such as summoning shareholdings' meeting to take relevant measures and/or withdrawing any proxy, pursuant to art. 2476 of C.C.

- **Measures against Statutory Auditors**

When the SB, Statutory Auditors and Board of Directors notice a breach of the Model by one or more Statutory Auditors, they shall promptly inform the Board of Directors, which in turn shall take all the necessary actions such as summoning shareholdings' meeting to take relevant measures.

- **Measures against members of the SB**

When the SB, Statutory Auditors and Board of Directors notice a breach of the Model by one or more members of the SB, they shall promptly inform the Board of Directors, which in turn shall take all the necessary actions such as withdrawing membership and appoints new members.

4.4.6. Disciplinary procedure for employees

The Company has adopted standard procedure to warn employees of disciplinary actions and charge relevant sanctions. Such procedure complies with the type, form and timing required by art. 7 of Employees' statute, applicable CCNL and any other legal and regulatory provisions.

Pursuant to par. 4.2, any potential breach of the Model and procedures must be promptly reported to the Chief Executive Officer, who (supported by relevant staff) shall assess the severity of the misconduct and the possibility to warn disciplinary actions.

In case of more severe sanctions than verbal warning, the Chief Executive Officer (supported by relevant staff) shall issue a written warning to the employee, who in turn shall provide all the relevant motivations within five days from the receipt of the warning.

Both written warning and any eventual motivation provided by the employee shall be promptly reported to the SB, which may express its opinion on the severity of the offence and applicable sanctions.

After five days from the issuance of the written warning, the Chief Executive Officer (supported by relevant staff) shall decide, after reading the opinion of the SB and the motivations of the employee, whether to impose any sanctions (written warning, suspension from work without salary up to six days, redundancy) commensurate to the severity of offences. The SB shall be promptly informed of any sanction imposed by the CEO.

Board of Directors and SB shall constantly monitor functioning and proper application of warning protocols and sanctions.

4.4.7. Sanctions to Recipients of report of possible wrongdoing ("Whistleblowing")

In order to preserve the identity of the whistleblower and prevent any possible retaliation or discrimination, the Company may impose the following sanctions to the subject entitled to receive any report of possible misconduct:

- ***Supervisory Body***

In the event of a breach of confidentiality on whistleblower perpetrated by one of the member, the other members shall promptly inform the Board of Directors, which in turn may withdraw the member and appoint a new one.

When the breach is perpetrated by the whole Supervisory Body, the Board of Directors shall withdraw all the members and appoint a new board, in accordance with relevant laws.

- ***Committee***

In the event of a breach of confidentiality on whistleblower perpetrated by one of the member, the Company shall apply relevant sanctions, as per par. 4.4.1, 4.4.3 and 4.4.4., commensurate to the severity of the offences.

4.4.8. Sanctions for third parties

Under a possible breach of the Model, the Company may:

- Warn the offender and impose (immediately or within a specific term) full compliance with its contractual duties, internal procedures and the Ethical Code;
- Claim a compensation for any damage suffered equal to the remuneration paid from the occurrence of the offence up to its resolution;
- Terminate immediately and automatically the contract for gross negligence, pursuant to art. 1453 and 1455 of C.C.

4.4.9. Register of offences

The company set a specific register for all the offences listed on par. 4.2, including offenders details and relevant sanctions imposed.

The register is kept by SNAITECH HR function and shall be constantly updated and made available to the SB, Board of Directors and Statutory Auditors.

When a third party is included in such register, it is no longer allowed to engage new relationships unless BoD authorise it.

5. Relationship with third party suppliers

Any written agreement related to collaboration and purchase of goods/services from third parties should include the following clauses:

- Reference to D.Lgs. n. 231/2001, where the third party supplier:
  - States to have received and read the Organisational, Management and Control Model and the Ethical Code;
  - Complies with the Organisational, Management and Control Model and the Ethical Code as long as theirs obligations and duties are compliant with relevant laws. Each party shall not induce to perpetrate any of the offences set forth by D. Lgs. no. 231/01;
  - Refrains from perpetration of any offence set forth by D. Lgs. no. 231/01.
- Intellectual property, where the parties agree on the following:
  - After the subscription of the agreement, any right and intellectual property shall remain to the original owner and the agreement, under no circumstances, entitles to transfer such rights;
  - Each party is the sole owner of all the rights and intellectual properties related to inventions, patents, brands, trade secrets and know-how on IT systems, proprietary software and any related manual even if developed and /or supported by the third party supplier;
  - Third party supplier agrees not to claim any intellectual property and rights owned solely by the other party and recognises full rights to profit from them;
  - Third party supplier acknowledges that any unauthorised access to IT systems and software of the other party – including algorithms and protocols – is persecuted as a breach of copyrights and may lead to criminal and civil sanctions.

6. Communication to and training of employees

Communication of the Model shall ensure full disclosure to reach all Recipients and inform them of any procedure and control to be followed when performing their duties and obligations.

SNAITECH ensures that all contents and principles of the Model must be disclosed to all Recipients and Third Parties when acting or contributing to achieve the Company's goals.

On this purpose, the Model and the Ethical Code are made available to all Senior Mangers, Employees reporting to Senior Managers and third parties on the company website, while they are made available on the intranet for all the remaining employees.

Third Parties are required to comply with the provisions of D.Lgs. no. 231/01 and the ethical principles of the Company by acknowledging the Model and its ethical principles.

Communication and training is supervised by the SB, which relies on relevant structures and functions to perform the following tasks:

- Promote any initiative to increase awareness and understanding of the Model, the contents of D.Lgs. 231/01 and its impacts on SNAITECH's business;
- Promote training and awareness of personnel to comply with principles of the Model;
- Promote and coordinate any initiative aimed at favouring awareness and understanding of the Model.

Training also focuses to increase awareness of D.Lgs. 231/01 and whistleblowing law with the aim to develop a proper corporate culture. Such awareness relies on providing and full disclosing the regulatory framework, the practical implications as well as principles and contents of the Model. All Senior Managers and Employees reporting to Senior Managers shall comply with such contents and principles.

A concrete awareness and understanding of the Model, Ethical Code and Internal Controls is ensured by specific mandatory training of Senior Mangers and Employees reporting to Senior Managers. Training shall be dispensed differently according to the Recipients and the training plan of the Company.

To ensure a widespread disclosure and effective knowledge of the current Model and the Ethical Code, the Company shall conducts precise communication and training of all recipients with the aim to inform them of all prescriptions and potential consequences of wrongdoing.

New hires shall be provided with an information package (including Ethical Code, Model, Decree, etc.), which provides basic knowledge useful to start working within the Company.

Contents and principles included in the General Section of the Model and the Ethical Code are also provided to third parties acting – also occasionally – to achieve the Company's goals.

It is responsibility of the Company to implement specific training plan to ensure real awareness of the Decree, Ethical Code and Model by any recipient.

Training on the Model is mandatory for all Recipients and is managed by HR function. The SB shall monitor the effectiveness of the training arranged by the HR function for all the recipients.

Different type of training (in terms of contents and modes) is provided according to the grade of recipients, level of risk associated with the activity and power of representation of the Company.

All training programs have a minimum common base including principles of D.Lgs. 231/01, offences under the Model and D.Lgs. 231/01 and any sensitive conduct, which may lead to offences.

Participation to training programs is mandatory and the Company shall have records of any training initiative and attendance, test level of understanding and appraisal of the course with the aim to develop new initiatives and improve the existing ones (through comments and suggestions on contents, materials, instructors, etc.). Any unjustified absence from training session leads to disciplinary actions.

Training may be provided online or based on IT systems and the SB supervises its contents. It should be provided by professional with relevant experience in the areas identified by the Decree. Any material shall be updated to reflect regulatory changes (for example the introduction of new offences) and Model changes (for example new Special Sections).

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D.LGS. NO. 231/01

Introduction to Special Sections

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premises

Pursuant to art. 6, par. 2, lett. a) of the Decree and based on the risk mapping process, the assessment of activities, existing controls and the business environment (*Control and Risk Self Assessment*), the Company has identified those sensitive activities (split by different type of offence) that may lead to possible offences set forth by the Decree.

To prevent or mitigate the risk of perpetrating these offences, the Company set general principles and conducts as well as general prevention protocols for all the sensitive activities and specific prevention protocols for each sensitive activity.

2. General prevention protocols

All recipients of the Model, as defined in par. 9 of the General Section, shall behave in compliance with laws, provisions of the current documents and principles of the Ethical Code. This is done in order to prevent possible offences set forth by the Decree.

In relation to all sensitive activities ruled by Special Sections, the general prevention protocols adopt the following principles:

- ✓ Only those subjects with previous authorisation may engage with officials from public administration;
- ✓ Any decision of the Company and its implementation shall adhere to principles and provisions included in the law, deed of incorporation and Ethical Code of the Company;
- ✓ Any responsibility of management, coordination and control of the Company are clearly stated and formalized;
- ✓ Grades, hierarchy as well as different duties within the Company are clearly stated and formalized;
- ✓ Authorizations for each action of the Company must be always recorded and proved;
- ✓ Proxy and power of attorney system is proportional to responsibilities of each director and any disclosure to third parties is ensured by adequate communication and information tools;
- ✓ Attribution and exercise of decision-making powers are balanced with the responsibilities and relevance/importance of business;
- ✓ There is segregation of duties between decision-makers, subjects involved in the accounting and subjects auditing and monitoring in accordance with laws and the internal control system;
- ✓ Any sensitive activity is implemented through procedures and guidelines. Also, it is identified an internal subject in charge of the activity (which usually matches with the head of function in charge of relevant sensitive activity). The individual in charge of the activity:
    - May ask information and clarifications to any corporate function, operational unit and individuals involved in the sensitive activity;

- Report promptly to the Supervisory Body of any critical issue or conflict of interest.

✓ Access to data of the Company is compliant with D.Lgs. no. 196 of 2003 and subsequent amendments and additions;

✓ Any document related to decisions and their implementation are stored by the relevant functions. Access to these documents is allowed only to authorised personnel as well as the Statutory Auditors, independent auditor and Supervisory Body;

✓ Selection of third party advisors shall me justified on the basis of their professionalism, independence and expertise;

✓ Any incentive plan for employees and collaborators shall be realistic and in line with duties, tasks performed and responsibilities;

✓ Any financial cash inflow and outflow of the Company shall be constantly monitored and tracked;

✓ Supervisory Body assesses full implementation of the general prevention protocols of this Special Section.

3. Layout of the Special Sections

Current Model is composed by 14 Special Sections each related to a macro-category of offence ex. D.Lgs. no. 231/01 and deemed applicable by the Company (see. Par. 2.12 "Relevant offences for SNAITECH S.p.A." of the General Section of the Model).

In particular, each Special Section covers:

- List of offences potentially referable to the Company;
- Areas and Divisional Heads potentially at risk (according to risk mapping);
- Sensitive Activities, which may potentially lead to crimes;
- Specific prevention protocols for each sensitive activity;
- Information flows to Supervisory Body;
- Disciplinary sanctions.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

D.LGS. N. 231/2001

Special Section A

Offences against the Public Administration (Artt. 24 e 25 D.Lgs. n. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise – Notions of "Public Administration", "Public Official" and " Person in Charge of Public Service"

The current Special Section refers to the offences set forth by articles 24 and 25 of D.Lgs. no. 231/01 ("**Offences against the Public Administration**") and, in particular, it rules the conduct held by directors and members of corporate governance bodies, managers and employees of SNAITECH as well as collaborators and external advisors, suppliers and other third parties when dealing, directly or indirectly, on a contractual or non-contractual basis (for example concessions, authorisations) with the Public Administration ("PA") and individuals acting of its behalf ("Recipients").

In summary, Public Administration refers to the overall system of public entities and individuals (State, Ministries, Regions, Provinces, Municipalities, etc.) and private legal persons with public functions, Public Administration of Foreign States as well as other entities classified by laws (concessioners, supervisory and control bodies, etc.)

Art. 357 of C.P. (Criminal Law) defines public official "*any individual holding a legislative, judiciary or administrative public office*" where "*public office includes any administrative function performed, through specific powers of attorney, on behalf on the Public Administration and ruled by public law and specific authorisations*".

Relevant 'public powers' include legislative, judicial and other powers of the 'administrative public function'.

Legislative power relates to the issuance of legal provisions (for example laws and decrees, etc.). Public Official performing a legislative public function includes any individual, at national or European level, empowered with this function. For example, public entities may include Parliament, Government, Regions, Provinces and other UE institutions with legislative powers.

Judicial power relates to the interpretation and application of laws to specific circumstances and it is usually exercised by those individuals directly involved in the judicial activity or related administrative activities. These individuals include magistrates, public prosecutors, members of the Justice Court and European Justice Courts.

Powers of the "***administrative public function"*** includes decision-making power, authoritative power and certification power:

- ***Decision-making power***: "*governing the decision making process of the Public Administration*" and any related activity. For example, the power of a committee to award participants in tendering processes;

- ***Authoritative power****:* any action taken by the Public Administration to achieve its goals. For example when a private individual is awarded with a license. On this purpose, any individual empowered with such power may be considered a "public official".

- ***Certification power***: any control and assessment by a public official aimed to confirm the existence of specific circumstances.

Differently, art. 358 of C.P. defines "*Person in Charge of a Public Service "* as *"any individual who performs public interest activities, not consisting of simple or merely material tasks, governed in the same manner as public function, but which do not entail the powers typically assigned to a Public Official*".

A Person in Charge of a Public Service usually performs a public function without any decision-making, authoritative and certification powers. For example, an employee of a private entity performing public services may be seen as a Person in Charge of a Public Service.

In public concessions usually the concessioner replaces and acts on behalf of the Public Administration when providing services or performing activity for the public interest. Therefore, the concessioner of a public service shall perform the institutional duties of the public entity issuing the concession.

SNAITECH S.p.A. is a concessioner of legal gambling activities (sports and horserace bets, online gambling) authorised by specific concession agreements awarded by Agenzia delle Dogane e dei Monopoli di Stato (ADM).

In particular, "Concessioner" relates to the concession of managing electronic network of gaming machines ex art. 110, par. 6, lett. a) e b) of TULS as well as retail and online gambling.

2. Offences set forth by 24 e 25 of D.Lgs. no. 231/01

An excerpt of the provisions of the Criminal Law included in art. 25 and 25 of the Decree is provided below along with a short comment.

- **Embezzlement to the detriment of the State (art. 316-*bis* of C.P.):**

"A subject, not part of the public administration, after lawfully receiving loans, subsidies or grants from the Italian Government or the European Union for the implementation of works or activities in the public interest, does not use the funds for the purposes for which they were granted, is punished with prison sentence from six months to four years".

This type of offence occurs when, after lawfully receiving loans, subsidies or grants from the Italian Government or the European Union for the implementation of works or activities in the public interest, a party does not use the funds for the purposes for which they were granted. The offence may be also related to funds received in the past and improperly allocated for different purposes.

- **Unlawful receipt of public grants to the detriment of the State (art. 316-*ter* of C.P.):**

"I. Unless the offence is ruled by art. 640-bis, any subject, by using or submitting false statements or documents, or by omitting due information, obtains grants, financing, subsidised loans or other similar contributions granted or issued by the State, by other Public Authorities or by the European Union without being entitled to them is punished with a prison sentence from six months to three years.

II. If the amount unlawfully received is lower than 3,999.96 Euro, then an administrative fine is exclusively applied and may range between 5,164 Euro and 25,822 Euro. However, the fine may not be larger than three times the amount unlawfully received."

The offence is committed when – by using or submitting false statements or documents, or by omitting due information – a party, not entitled to, receives grants, financing, subsidised loans or other similar contributions granted or issued by the State, by other Public Authorities or by the European Union.

- **Extortion in office (art. 317 of C.P.):**

"A Public Official or a Person in Charge of a Public Service who, abusing of his/her office or powers, forces someone to give or promise to him/her or a third party money or other undue benefits is punished with a prison sentence between six to twelve years".

The offence is perpetrated when a Public Official or a Person in Charge of a Public Service who, abusing of his/her office or powers, forces someone to give or promise to him/her or a third party money or other undue benefits.

- **Bribery relating to the exercise of duties (art. 318 of C.P.):**

"A Public Official who receives, for his/her own benefit or for the benefit of others, money or other benefits, or accepts a promise thereof, for performing his/her own duties or exercising his/her own powers is punished with a prison sentence between one to six years".

This type of offence occurs when a Public Official or a Person in Charge of a Public Service (when acting as a public employee as per art. 320 C.P.) receives, for his/her own benefit or for the benefit of others, money or other benefits, or accepts a promise thereof, for performing his/her own duties or exercising his/her own powers.

The funds used for bribery may be taken, for example, from:

- ✓ Black funds from issuing invoices related to non-existing transactions;
- ✓ Reimbursements of fictitious or grossed up expenses, also related to advisory activities.

Other examples of bribery may include gifts, hiring personnel or selection of suppliers sponsored by the Public Official.

- **Bribery relating to an act contrary to official duties (articles 319 – 319-*bis* of C.P.):**

  - **Art. 319 of C.P. - Bribery relating to an act contrary to official duties:**

    "A Public Official who omits or delays an act, to be performed or already performed, that is contrary to the official duties of a public agent against receiving undue payment or benefits is punished with prison sentence from six to ten years".

  - **Art. 319-bis of C.P. – Aggravating circumstances:**

    "The sanction is more severe when the offence of art. 319 related to public funds, salary, pension contributions, tax payments, reimbursements or execution of contracts with the public administration represented by the culpable public official".

    This type of offence occurs when a Public Official or a Person in Charge of a Public Service receives money or other benefits for performing, or having performed, any acts contrary to the

official duties or when omitting/delaying, or having omitted/delayed, any act of his/her official duties.

- **Bribery in judicial proceedings (art. 319-*ter* of C.P.):**

"I. When the offences ruled by articles 218 and 219 are committed to favour or damage one of the parties to a criminal, civil or administrative proceeding, then a prison sentence between six and twelve years shall apply.

II. In a case of undue prison sentence under five years, the offender is punished with a prison sentence between six and fourteen years; if undue sentence is above five years or life sentence than the offender is punished with prison sentence between eight and twenty years".

In this type of offence, the conduct of the bribed person and the bribe-giver (ruled by articles 318 and 319 of C.P.) is characterised by the specific aim of favouring or damaging one of the parties to a criminal, civil or administrative proceeding.

For example, during a judicial proceeding (eg. in civil proceeding to receive compensations for damages, forced execution of a contract or in criminal or administrative proceeding related to a contested trade licence), the Company may be liable, when a director or an employee bribes a Public Official (judge, chancellor, technical expert) in order to obtain a favourable sentence or reduce any negative impact of the sentence.

- **Illegal inducement to give or promise benefits (Art. 319-*quater* of C.P.):**

"I. Unless the offence relates to a more severe crime, a person in charge of a public service or a public official who, abusing of his/her office or powers, induces another person to give or promise to him/her or to a third party money or other undue benefits is punished with prison sentence between six and ten years and six months.

II. If the offender makes or promises any money or other benefits then is punished with a prison sentence up to three years".

The offence is committed when money or other benefits are promised or corresponded to a Public Official or a Person in Charge of a Public Service, even if the latter induced the offender to promise or pay.

- **Bribery of a person in charge of a public service (art. 320 of C.P.):**

"I. Provisions of articles 318 and 319 apply to persons in charge of public service as well.

II. In any case, the sanctions are reduced by no more than one third".

As previously mentioned, bribery, as per art. 318 and 319, is committed also when a Person in Charge of a Public Service receives, for his/her own benefit or for the benefit of others, undue money or other benefits for performing his/her own duties or acting against his/her duties.

- **Sanctions for the bribe giver (art. 321 of C.P.):**

"Sanctions in the first paragraph of art. 318, 319, 319-bis, 319-ter and 320 related to offences set forth by articles 318 and 319 are applicable also to individuals promising or corresponding money and other benefits to a public official or a person in charge of a public service".

Given the specific nature of bribery and its joint responsibility, pursuant to art. 320 of C.P., the sanctions of art 318, par. 1, 319, 319-bis, 319-ter and 320 of C.P. apply also in those circumstances where the briber giver is an individual close to the Entity.

- **Incitement to bribery (art. 322 of C.P.):**

"I. If there is a rejection of an offer or promise of undue money or other benefits made to a public official or a person in charge of public service for performing his/her duties or exercising his/her own powers, then the sanction in art. 318 is reduced by one third.

II. If there is a rejection of an offer or promise made to a public official or a person in charge of public service to induce the omission or delay of an act, to be performed or already performed, that is contrary to the official duties of a public agent, then the sanction in art. 319 is reduced by one third.

III. The sanction in first paragraph is imposed to the public official or person in charge of public service who induces, by promising or offering money or other benefits, to perform his/her duties or powers.

IV. The sanction in first paragraph is imposed to the public official or person in charge of public service who, through a private party, induces, by promising money or other benefits, to achieve purposes of art. 319".

The offence occurs when there is a rejection of an offer or promise made to a Public Official or a Person in Charge of Public Service for performing his/her duties.

When the rejection relates to offers or promises made to a public official or a person in charge of public service to induce the omission or delay of an act, to be performed or already performed, that is contrary to the official duties of a public agent, then the sanction in art. 319 is reduced by one third.

- **Peculation, extortion, illegal inducement to give or promise benefits, bribery and incitement to bribery of members of international criminal courts, EU institutions and foreign States (Art. 322-bis of C.P.):**

  "I. Provisions of articles 314, 316, 317 to 320 and 322, third and fourth paragraph shall apply also to:

  1) Members of EU Commission, Parliament, Justice Court and Court of Auditors;

  2) Officials and employees of European Community;

  3) Persons, within member States or other public or private entity within the European Community, holding corresponding functions of official and employees of European Community;

4) Members and employees of entities established on the basis of the founding Treaties of the European Community;

5) Persons of EU member States holding corresponding functions or performing corresponding activities of public officials and persons in charge of public service;

5bis) Judges, prosecutor, adjunct prosecutors, officials and employees of international criminal court, persons responding to member States of the Treaty establishing the international Criminal court holding corresponding functions of officials of the Court, members and employees of entities established on the basis of the founding Treaty of the international Criminal court.

II. Provisions of articles 319-quarter, par. 2, 321 and 322, first and second paragraphs, apply as well if the money or other benefit is offered or promised to:

1) Persons listed in the current articles;

2) Persons holding corresponding functions or performing corresponding activities of public officials and persons in charge of a public service within foreign Sates and public international organisations as long as the offence is committed during an international transaction.

III. Persons listed in the first paragraph are considered similar to public officials, when performing corresponding functions, and similar to persons in charge of public service in all the other circumstances.

The offence occurs when one of the aforementioned conducts is directed to members of European Community and foreign States bodies. On this purpose, bribery is committed also when directed to foreign subjects, according to the Italian law, linked to Public Officials and Persons in Charge of Public Service.

- **Fraud against the State or another public entity or European Community (art. 640, par. 2 of C.P.):**

  "I. A subject obtaining unfair profit and causing damages to third parties by means of artifices or deceits aimed at misleading, is punished with prison sentence from six months to three years and a fine from 51 Euro to 1,032 Euro.

  II. The prison sentence ranges from one to five years and the fine ranges from 309 Euro and 1,549 Euro when:

  1. The offence is perpetrated against the State or other public entity or aimed at avoiding the army service;

  2. The offended person was threatened with a fictitious danger or induced to believe to perform a specific order from an authority.

  2-bis The offence is committed under circumstances of art. 61, num. 5).

  III. The offence is punished following a compliant made by the offended person unless one of the previous circumstances apply or an aggravating circumstance applies".

This type of offence occurs when an unfair profit is obtained by means of artifices or deceits aimed at misleading and causing damage to the State or any other Public Body. This offence occurs, for instance, when, false information supported by forged documents are provided to public officials and relevant employees.

- **Aggravated fraud for the purpose of obtaining public funds (art. 640-*bis* of C.P.):**

"If the offence sets forth by art. 640 is carried out for the purpose of unduly obtaining public funds from the State, other public entities and European Community, the prison sentence is from one to six years".

This type of offence occurs when the fraud, mentioned on previous point, is carried out for the purpose of unduly obtaining public funds from the State, other Public bodies or the European Union.

- **Computer fraud against the State or other public entity (art. 640-*ter* of C.P.):**

"I. A subject obtaining unfair profit and causing damages to third parties by means of altering the functioning of an IT or telecommunication system or tampering with the data or software contained therein, is punished with a prison sentence from six months to three years and a fine from 51 Euro to 1,032 Euro.

II. The prison sentence ranges from one to five years and fine ranges from 309 Euro and 1,549 Euro when one of the circumstances in art. 640, num. 1, par. 2 applies or the offence is perpetrated by the manager of the electronic system.

III. The offence is punished following a compliant made by the offended person unless one of the circumstances under par. 2 apply or an aggravating circumstance applies".

The offence consists of two different alternative misconducts: altering the functioning of an IT or telecommunication system or tampering with the data or software contained therein, also with the support of other individuals, with the aim to obtain unfair profit from the Public Administration.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal;
- Occupational Health and Safety;
- Information Technology;
- Administration, finance and Internal Audit;
- Communication and promotions;
- Compliance;
- Procurements of goods and services;
- HR.

4. Sensitive activities related to offences against the Public Administration

From the analysis conducted by SNAITECH within each Division and Unit, the activities potentially exposed to perpetration of offences may be classified as follows:

- Activities exposed to "***direct risk of perpetrating the offence***" such as activities involving direct relationships with Public Officials and Persons in Charge of Public Service. These activities may lead to perpetrate one or more crimes against the Public Administration;

- Activities that may "***contribute to perpetrating an offence***" against the Public Administration. These activities are related to management of financial instruments and therefore may be functional to generate black funds.

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to offences against the Public Administration, pursuant to articles 24 and 25 of the Decree:

- ✓ Management of relations, communications and duties required by supervisory authorities and public entities (Consob, GdF, AdE, Ministry of Economic Development, Ministry of Agriculture, UIF, Provincial Division of Labour, Labor inspectorate, INPS, INAIL, Technical offices of Municipalities, etc.);

- ✓ Management of tender participation to gambling concessions;

- ✓ Management of the activities relating to the request for authorisation or fulfilment of requirements towards the public administration (e.g. NOE, CIV, POS building renovation permits, DIA, SCIA, etc.);

- ✓ Acquisition and/or management of public subsidies/contributions/funds (e.g. Ministry of Agriculture)

- ✓ Relations and activities with public officials and/or persons in charge of public service (e.g. ADM, GdF, AdE, MIPAAF, ASL, NAS, Technical offices of Municipalities, Labor inspectorate, INPS, INAIL, etc.), also through external advisors, during: inspections, controls and assessments;

- ✓ Selection and management of agents;

- ✓ Management of incentives paid to the distribution network (e.g. Additional compensation and bonus);

- ✓ Management and assessment of compliance with gambling parameters and proper functioning of gambling activities (compliance with ADM regulation);

- ✓ Management of terminals instalment and set up (roll-out and connectivity);

- ✓ Periodic inspections to verify compliance with concessions (AWP, VLT, ads);

- ✓ Management of the procedures for the procurement of goods and services (including screening of suppliers);

- ✓ Management of the procedures for the appointment of professional consultants (including screening and other relations (also of legal nature) with consultants);
- ✓ Disclosure of mandatory information pursuant to D.Lgs. 58/07 and Issuers' Regulation (corporate releases and privileged information);
- ✓ Management of direct and indirect taxation;
- ✓ Treasury activities including cash movements of bank accounts;
- ✓ Management and recording credit and debit invoices and receipts;
- ✓ Screening, hiring and management of personnel (also indirectly through third parties);
- ✓ Management of corporate incentives and benefits;
- ✓ Management of business trips, advance payments and reimbursement of travel expenses;
- ✓ Management of information flows to Public Administration by means of IT tools (PEC, ADM platform, AdE platform for e-invoice, etc.);
- ✓ Access to systems and authorisation to change information and data stored in the Company records (accounting, personnel, suppliers, clients, PEP, etc.);
- ✓ Management of sponsorships and donations;
- ✓ Management of gifts;
- ✓ Management of entertainment expenses;
- ✓ Management of relations with judicial authorities during litigations (fiscal, administrative, civil, labour and appeals against the entity issuing the concession).

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Specific prevention protocols

Transactions related to **Management of relations, communications and duties required by supervisory authorities and public entities (Consob, GdF, AdE, Ministry of Economic Development, Ministry of Agriculture, UIF, Provincial Division of Labour, Labor inspectorate, INPS, INAIL, Technical offices of Municipalities, etc.); Management of the activities relating to the request for authorisation or fulfilment of requirements towards the public administration (e.g. NOE, CIV, POS building renovation permits, DIA, SCIA, etc.); Disclosure of mandatory information pursuant to D.Lgs. 58/07 and Issuers' Regulation (corporate releases and privileged information); Management of direct and indirect taxation; Management of information flows to Public Administration by means of IT tools (PEC, ADM platform, AdE platform for e-invoice, etc.); Access to systems and authorisation to change information and data stored in the company records (accounting, personnel, suppliers, clients, PEP, etc.)**. Protocols include the following steps:

- ✓ Any document, request and formal communication to PA must be managed and signed only by those subjects with relevant powers entrusted by internal rules;

- ✓ These subjects shall inform his/her line and functional manager of any meeting with PA as well as of any key outcome of the meeting;

- ✓ The subject in charge and responsible for the transaction shall:

  - Identify the most suitable instruments used by his/her Function when dealing with PA and ensure that relations are always transparent, recorded and verifiable;

  - Authorise preliminary the use of any data or information on the Company when reporting documents, requests and communications to PA;

  - Assess completeness and accuracy of any document, statement and information provided to PA by the Company;

- ✓ Any subject enabled to access IT systems (used to interact with PA) shall be clearly identified;

- ✓ Verify any password held by employees to log on IT systems used to deal with PA;

- ✓ Monitoring of compliance with legal provisions, with the aim of filing timely any income statement and/or other fiscal statements;

- ✓ The person in charge of the relevant Function shall store any documentation such that any further amendment is allowed only with specific authorisation and relevant evidence is provided (in order to ensure proper traceability of the process and facilitate any eventual subsequent control).

- ✓ Transactions related to: **management of tender participation to gambling concessions; periodic inspections to verify compliance with concessions (AWP, VLT, ads)**. Protocols include the following steps:

- ✓ Setting up specific procedures for activities, roles, responsibilities and controls when participating to tender procedures;

- ✓ Fairness and completeness of the documents presented (technical requirements, economic requirements, etc.) is assessed, also with specific controls;

- ✓ It is formally appointed any subject authorised to deal with relevant entities holding an auction;

- ✓ Any relations and communication with PA in the contest of tender procedure is formalised and stored;

- ✓ There is segregation of duties between subjects who arrange, verify, authorise and sign documents required by the PA;

- ✓ Responses to tender procedures on concessions must be systematically reviewed and authorised by relevant attorneys;

- ✓ Verifying compliance with the tender procedure of any terms, requirements and conditions;

- ✓ Documents related to tender procedures are systematically stored;

- ✓ Verify any password held by employees to log on IT systems used to deal with PA;

- ✓ Board of Directors shall assess and approve participation in tender procedures;

- ✓ Any document required by the tender procedure is signed by the Chief Executive Officer or other relevant attorneys;

- ✓ Monitoring systematically the compliance with requirements of concessions award/renewal.

Transactions related to the **acquisition and/or management of public subsidies/contributions/funds (e.g. Ministry of Agriculture)**. Protocols include the following steps:

- ✓ Setting up criteria and procedures to assess eligibility to receive subsidies, funds, etc.;

- ✓ Identifying person in charge, entrusted with power of attorney, who acts on behalf of the Company or coordinates any eventual external professionals;

- ✓ Any request of subsidies, funds, etc. shall be preliminary authorised and signed in accordance with internal proxy, procedures and authorisation systems;

- ✓ The subject in charge of the transaction shall assess the completeness and accuracy (in terms of economic and financial information provided) of any documents submitted to obtain funds, subsidies, etc.

- ✓ Financial resources received are addressed and used exclusively for the purposes specified in the request;
- ✓ Any use of funds shall always be justified by the applicant by certifying the coherence of his/her request with the purposes of the funds received by the Company;
- ✓ Persons in charge of the relevant Functions involved in the transaction shall store any documentation in order to ensure proper traceability of the process and facilitate any eventual subsequent control.

Transactions related to **relations and activities with public officials and/or persons in charge of public service (e.g. ADM, GdF, AdE, MIPAAF, ASL, NAS, Technical offices of Municipalities, Labor inspectorate, INPS, INAIL, etc.), also through external advisors, during: inspections, controls and assessments.** Protocols include the following steps:

- ✓ It is formally appointed any subject authorised to deal with Public Administration during inspections;
- ✓ Setting up responsibilities and procedures to manage relations with Public Administration during inspections of Points of Sales;
- ✓ At least two subjects (identified previously) shall attend inspections of the company's premises;
- ✓ Setting up procedures to make suitable structures (such as detachable offices, access to network, hardware) available for inspectors and provide them with any corporate documentation needed;
- ✓ Persons in charge shall promptly inform the SB of the beginning and conclusion of the inspections as well as of any critical issue raised, including the following information:
  - Contact details of inspectors (name and entity);
  - Date and time of arrival;
  - Length of the inspection;
  - Purpose of the inspection;
  - Outcome of the inspection;
  - Report issued by the entity running the inspection;
  - List of documents provided to inspectors.
- ✓ SB shall store any documentation such that any further amendment is allowed only with specific authorisation and relevant evidence is provided (in order to ensure proper traceability of the process and facilitate any eventual subsequent control).
- ✓ Define clearly mitigants and remedial actions to critical issues discovered during the inspections by public official or persons in charge of public service. Furthermore, the effective implementation of mitigants and remedial actions shall be monitored using inspections.

For transactions related to: **selection and management of agents; screening, hiring and management of personnel (also indirectly through third parties)**. Protocols include the following steps:

- ✓ Any Function seeking to hire personnel shall fill and submit relevant forms. The hiring must be compliant with the limits of annual budget;
- ✓ Hiring request is authorised by the relevant person in charge;
- ✓ Any hiring request out of the budget limits shall be justified and authorised in compliance with procedures and internal controls of the Company;
- ✓ Each hiring process shall include at least three candidates, unless the peculiarity of the position does not allow to find candidates;
- ✓ Candidates are interviewed and evaluated also according to their ethic and attitudes;
- ✓ Candidate assessment shall be formalised and reported in specific documents stored by the relevant Divisional head;
- ✓ Any relation, direct or indirect, with the PA is preliminary verified;
- ✓ Resigned employees shall be interviewed as well.

Transactions related to the **management of incentives paid to the distribution network (e.g. Additional compensation and bonus)**. Protocols includes the following steps:

- ✓ Verifying the eligibility of the request;
- ✓ The request of incentives is in line with the budget and the development plan of the Company;
- ✓ Payment of incentives is authorised by relevant attorneys;
- ✓ Monitoring any incentive paid to PoS to ensure its compliance with the purposes and authorisation provided.

Transactions related to: **management and assessment of compliance with gambling parameters and proper functioning of gambling activities (compliance with ADM regulation); management of terminals instalment and set up (roll-out and connectivity)**. Protocols includes the following steps:

- ✓ Setting up clearly roles and responsibilities of the relevant functions involved;
- ✓ Ethical Code shall encourage and inspire any conduct to be compliant with criteria of fairness, transparency and integrity when dealing with PA;
- ✓ Ethical Code shall prohibit offering undue payments or other benefits to public officials;
- ✓ It is appointed a person in charge of managing relations, communication and other requirements from entities releasing concessions (AAMS, Ministry of Economic Development, Ministry of Agriculture, etc.);

- ✓ It is appointed a person in charge of managing relations, communication and other requirements needed to obtain authorisations and licences for the business;
- ✓ Periodic inspections of PoS to assess the legality of any gambling activity performed;
- ✓ It is appointed a person in charge of supervising the integrity of gambling parameters (in relation to his/her business line).

Transactions related to the **management of the procedures for the procurement of goods and services (including screening of suppliers)**. Protocols include the following steps:

- ✓ There is segregation of duties between subject who authorises purchases and files the order to the supplier;
- ✓ Any documentation related to the purchase shall include information on the procedures followed for order, its object, amount and justification behind the selection of supplier;
- ✓ Any purchase of goods and services is ruled by contracts or written orders with precise indications of prices and relevant criteria to assess it;
- ✓ There must be a relevant number of offerings in order to select suppliers;
- ✓ When selecting a supplier, preliminary controls shall be conducted to assess and monitor technical, organisational and managerial skills as well as ethical, economical and financial reliability;
- ✓ The person in charge of the function involved in the purchase shall promptly inform the SB of any critical issue in the services provided by the suppliers or any specific requests received by the suppliers;
- ✓ Contracts related to the supply of goods and services shall include specific clauses and liabilities to comply with contractual obligations and shall adhere to the principles of Ethical Code and Model;
- ✓ Any payment to suppliers shall be made after preliminary authorisation by the person in charge of the function involved in the purchase and shall follow the internal authorisation procedure, which takes into account any eventual deadline of the payment;
- ✓ Any use of financial resources shall be clearly justified and recorded in compliance with the principles of professional and accounting fairness;
- ✓ Any invoice of goods and services purchased shall be recorded once there is a clear evidence of goods received or the services provided;
- ✓ There is segregation of duties between the subject who authorises, controls and implements the transactions.

For transactions related to **management of the procedures for the appointment of professional consultants (including screening and other relations (also of legal nature) with consultants)**. Protocols include the following steps:

- ✓ Advisors shall be selected according to their professionalism, independency and expertise;
- ✓ The selection shall be justified by the corporate function making the request;
- ✓ The appointment shall be compliant with the procedures, authorisations and internal controls of the Company and shall be in line with the budget and the nature of services required;
- ✓ There is segregation of duties between the subject who authorises and appoints the advisor;
- ✓ Mandate shall be in writing and include information on the remuneration and nature of service;
- ✓ Contracts with advisors shall include the following clauses:
  - A specific acknowledgement statement of the provisions of the Decree, Ethical Code and the Model as well as a commitment statement to adhere with fundamental principles;
  - Any contractual breach is subject to the provisions mentioned in previous point;
- ✓ If there is no evidence of the service provided, the Consultant shall detail all the activities and services provided at the end of the mandate;
- ✓ The relevant function shall assess the successful performance before authorising any payment;
- ✓ It is forbidden to set remuneration not in line with the services provided to the Company, the mandate, market practices or professional rates set for the relevant advisory activities.

For transactions related to: **treasury activities including cash movements of bank accounts; management and recording credit and debit invoices and receipts**. Protocols include the following steps:

- ✓ Narrow any independent use of financial resources by setting up specific threshold in line with skills and responsibilities. Exceeding such limits may be justified only for urgent and exceptional reasons: in such circumstances the breach shall be duly authorised afterwards;
- ✓ The Board of Directors or the relevant attorney establishes and changes, if needed, the procedure for the joint signature of specific transactions above the threshold;
- ✓ There is segregation of duties between the subject who authorises and makes the payment to third parties;
- ✓ Any use of financial resources shall be clearly justified and recorded in compliance with the principles of professional and accounting fairness;
- ✓ Any use of financial resources shall be justified by the relevant applicant also by providing the nature of the expenses to be sustained;

- ✓ It is forbidden any cash payment or collection but small expenses duly authorised by the relevant functions;
- ✓ The Company may deal only with financial institutions subject to specific EU regulations on fairness and transparency;
- ✓ Setting up specific limits to advanced payments and reimbursements of employees' expenses. Any reimbursement must be claimed by filing specific forms and providing relevant invoices or receipts.

For transactions related to the **management of corporate incentives and benefits**, protocols include the following steps:

- ✓ Setting up an adequate benefit system which relies on proportionality criteria and is in line with goals achieved;
- ✓ Goals must be legal and may be of economic and qualitative nature;
- ✓ There is segregation of duties between the subject who authorises and controls the benefits attribution;
- ✓ There must be an annual assessment of skills and goals achieved by employees, in order to consider any change of grade and benefits;
- ✓ Any incentive and benefit to employees and collaborators shall be in line with duties, responsibilities and activities performed;
- ✓ The Divisional Head shall store any documentation such that any further amendment is allowed only with specific authorisation and relevant evidence is provided (in order to ensure proper traceability of the process and facilitate any eventual subsequent control).
- ✓ The attribution of specific corporate assets shall be justified according to the role and duties of the beneficiary employee. It may be required by filing formal request and authorised by a line manager according to the provisions of the Model;
- ✓ Setting up procedures to request and authorise any corporate assets and benefits;
- ✓ Identify all the corporate assets and benefits attributed (e.g. laptop, mobile phone, etc.);
- ✓ Maintaining and updating the inventory of any asset attributed;
- ✓ Establish withdrawal rules for breaches of corporate rules and procedures;
- ✓ Setting up procedures for assets return in case of redundancy/resignation.

For transactions related to: **management of business trips, advance payments and reimbursement of travel expenses**; **management of entertainment expenses**. Protocols include the following steps:

- ✓ Reimbursement of travel and entertainment expenses must be claimed by filing a specific form and providing relevant invoices or receipts;
- ✓ It is appointed, according to the hierarchy levels within the Company, the person in charge of authorising reimbursement forms *ex ante* or *ex post* (depending if the business trips is on unusual locations);
- ✓ Travel and entertainment expenses shall be managed in line with internal policies, purposes of expenses, authorisations and relevant payments.

For transactions related to: **management of sponsorships and donations**; **management of gifts**. Protocols include the following steps:

- ✓ Sponsorships, donations and gifts shall have maximum thresholds set by the Company;
- ✓ Transactions shall be legal and ethical and duly authorised, proved and justified with full description of goods/services offered and their values;
- ✓ Transactions shall enhance and promote the culture and image of the Company;
- ✓ It is produced an annual report of all sponsorships and donations;
- ✓ Transactions must be verifiable and traceable through proper recording.

For transactions related to the **management of relations with judicial authorities during litigations (fiscal, administrative, civil, labour and appeals against the entity issuing the concession)**. Protocols include the following steps:

- ✓ It is always appointed a person, entrusted with relevant power of attorney, to act on behalf of the Company and coordinate any eventual external advisors;
- ✓ Relations with Judicial Authority and PA during a judicial or non-judicial litigation shall be inspired by principles of fairness, transparency and traceability, also when managed by external advisors;
- ✓ The person in charge shall inform the SB of the beginning of the litigation, any step taken and the final sentence as well as any critical issue raised;
- ✓ It shall be tracked any request of information, person involved and authorising documentation to be provided in the litigation;
- ✓ The person in charge of the relevant function shall store any documentation in order to ensure proper traceability of the process and facilitate any eventual subsequent control.

6. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D.LGS. N. 231/01

Special Section B

Corporate offences
(Art. 25-ter D.Lgs. n.231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

The current Special Section refers to the offences set forth by article 25-ter of D.Lgs. no. 231/01, introduced by D.Lgs. no. 61 of 11 April 2002 and subsequent amendments and additions.

In particular, it rules the conduct held by those subjects – directors, managers and employees of SNAITECH as well as collaborators, external advisors and suppliers performing their services within the Company regardless the legal nature of their relationship with the Company – involved in the process and sensitive activities ("Recipients").

All Recipients of the current Special Section of the Model shall behave in compliance with the following provisions, in order to prevent the perpetration of any crime set forth by relevant laws.

2. Offences of art. 25-*ter* of D.Lgs. no. 231/01

Article 25-*ter* of D.Lgs. no. 231/01 includes the following corporate offences:

- False corporate reporting (art. 2621 of c.c.);
- Minor events (art. 2621-*bis* of c.c.);
- False corporate reporting by listed companies (art. 2622 of c.c.);
- Obstruction of controls (art. 2625 of c.c.);
- Undue repayment of contributions (art. 2626 of c.c.);
- Unlawful distribution of profits and reserves (art. 2627 of c.c.);
- Unlawful dealing in the stocks or shares of the company or its parent company (art. 2628 c.c.);
- Transactions prejudicial to creditors (art. 2629 of c.c.);
- Failure to disclose conflicts of interest (art.2629– *bis* of c.c.)
- Capitalising fictitiously (art. 2632 of c.c.);
- Improper distribution of the company's assets by its liquidators (art. 2633 of c.c.);
- Bribery among private individuals (art. 2635 of c.c.);
- Instigating bribery among private individuals (art. 2635-bis of c.c.);
- Unlawfully influencing the shareholders' meeting (art. 2636 of c.c.);
- Market rigging (art. 2637 of c.c.);
- Obstruction of the duties of the Public Supervisory Authorities (art. 2638 of c.c.).

For each of the above listed offences, it is provided an excerpt of the provisions along with a short comment.

- **False corporate reporting (art. 2621 of c.c.):**

"Excluding the offences ruled by art. 2622, the directors, general managers, director in charge of the accounting reports, statutory auditors and insolvency practitioners, with the aim to achieve unfair gains for themselves or other parties, consciously represent untrue facts or omit to disclose material facts in the financial statements, reports and other corporate documents of the company or the group and such representation may concretely mislead the intended recipients. These offenders are punished with prison sentence from one to five years.

The same sanction applies also if the illegal act refers to assets held or administered by the company on behalf of third parties".

After the introduction of Law no. 69 of 27 May 2015, the sanction was changes from fine to prison sentence from one to five years applicable to those directors, general managers, director in charge of the accounting reports, statutory auditors and insolvency practitioners who represent untrue facts or omit material facts in the financial statements, reports and other corporate documents of the company or the group.

Furthermore:

- Corporate documents include any communication to shareholders and general public such as financial statements, reports, disclosures pursuant to articles 2501-ter and 2504-novies c.c. in the event of merger or split and pursuant to art. 2433-bis c.c. in the event of interim dividends;

- The concept of misleading other parties put emphasis on the real risk of the offence;

- The recent deletion (by Law 69/15) of "*subject to assessment*" in the article, when referring to untrue facts, expresses the intention of legislator not to give criminal relevancy to the activity of "pure" assessment;

- The unlawful conduct is perpetrated with the aim of obtaining unfair profits for the perpetrator or others;

- Untrue or undisclosed facts must be material and potentially able to change significantly the representation of economic and financial situation of the company or the group;

- The introduction of "*consciously*" put emphasis on the awareness of perpetrator to represent untrue facts or avoid disclosure of material information;

- The same prison sentence from one to five years applies also if the illegal act refers to assets held or administered by the company on behalf of third parties.

- **Minor offences (art. 2621-*bis* of c.c.):**

"Unless a major crime is committed, the prison sentence is reduced, from a minimum of six months to a maximum of three years, when conducts of art. 2621 are considered minor offences on the basis nature and scale of the company and consequences produced by the unlawful conducts.

Unless a major crime is committed, the same sanction of the previous paragraph applies when conducts of art. 2621 refer to companies below the limits of the art. 1, par. 2 of Royal Decree no.

276 of 16 March 1942. In this case, the offence is punishable upon request and complaint by the company, shareholders, creditors and other recipients of the corporate disclosure".

The article envisages false corporate reporting also for minor offences with a reduction of sanctions (from six months to three years of prison sentence). The sanction applies as well to those companies not subject to the bankruptcy law.

The Court will assess whether the offence is minor given the nature and scale of the company and the consequences produced by unlawful conduct.

The Court may not judge directly such offence unless a formal compliant is filed by the offended party (company, shareholders, creditors and other recipients of the corporate disclosure).

- **False corporate reporting by listed companies (art. 2622 c.c.):**

"Directors, general managers, director in charge of the accounting reports, statutory auditors and insolvency practitioners of companies issuing financial instruments listed on regulated Italian or other European markets, with the aim to obtain unfair gains for themselves or other parties, consciously represent untrue facts or omit to disclose material facts in the financial statements, reports and other corporate documents of the company or the group and such representation may concretely mislead the intended recipients. These offenders are punished with prison sentence from three to eight years.

The companies of the previous paragraph include:

1) *Companies issuing financial instruments whose listing application for a regulated Italian or other European markets has been submitted;*

2) *Companies issuing financial instruments listed on an Italian multi trading facility;*

3) *Parent companies of undertakings issuing financial instruments listed on a regulated Italian or other European markets;*

4) *Companies collecting or managing savings.*

The same sanction applies also when the illegal act refers to assets held or administered by the company on behalf of third parties".

The article was changed following the introduction of Law no. 69 of 27 May 2015 by removing the wording "*untrue corporate disclosure to damage shareholders and creditors*" instead of the untrue corporate disclosure perpetrated by listed companies or similar companies as per par. II.

Prison sentence (from three to eight years) applies to directors, general managers, director in charge of the accounting reports, statutory auditors and insolvency practitioners of companies issuing financial instruments listed on regulated Italian or other European markets, who, with the aim to obtain unfair gains for themselves or other parties, consciously represent untrue facts or omit to disclose material facts in the financial statements, reports and other corporate disclosures of the company or the group and such representation may concretely mislead the intended recipients.

Furthermore:

- Corporate documentation includes any communication to shareholders and general public such as financial statements, reports, disclosures pursuant to articles 2501-ter and 2504-novies c.c. in the event of merger or split and pursuant to art. 2433-bis c.c. in the event of interim dividends;
- The concept of misleading other parties put emphasis on the real risk of the offences;
- The unlawful conduct is perpetrated with the aim of obtaining unfair profits for the perpetrator or others;
- Untrue or undisclosed facts must be material and potentially able to change significantly the representation of economic and financial situation of the company or the group;
- The recent deletion (by Law 69/15) of "*subject to assessment*" in the article, when referring to untrue facts, expresses the intention of legislator not to give criminal relevancy to the activity of "pure" assessment;
- The introduction of "*consciously*" put emphasis on the awareness of perpetrator to represent untrue facts or avoid disclosure of material information;
- The introduction of Law no. 69/15 deleted the existence of any pecuniary damage for the company, shareholders or creditors; the offence is punishable, given its danger, regardless the existence of such pecuniary damage.

The offence may be perpetrated in the interest of the company, for example by creating black funds through undervaluation of assets or overvaluation of liabilities in order to self-finance or cover any losses incurred during the period.

- **Obstruction of controls (art. 2625 of c.c.):**

"Directors, who conceal documents or otherwise act so as to prevent or hinder shareholders or other corporate governance bodies to perform their controls, are punished with a fine up to 10,329 Euro.

If the unlawful conduct damaged shareholders, then the sanction may include prison sentence up to one year if the offended party files a formal complaint.

The sanction is doubled if the company has financial instruments listed on Italian or other European markets or the instruments are mainly sold to the generic public pursuant to art. 116 of D. Lgs. no. 58 of 24 February 1998".

Paragraph 1 punishes with an administrative sanction the conduct to prevent or hinder shareholders or other corporate governance bodies from performing their controls (for example statutory auditors).

In the event that shareholders are damaged by the unlawful conduct, then a criminal sanction is introduced by paragraph 2.

This is a typical offence of directors and the generic fraudulence is a necessary and sufficient condition.

- **Undue repayment of contributions (art. 2626 of c.c.):**

"*Excluding those circumstances of legal share capital reductions, directors, who repay shareholders' contributions, also by means of simulated transactions, or exempt shareholders from the obligation to make such contributions, are punished with a prison sentence up to one year".*

The article rules a fraudulent offence perpetrated by directors and preserves the integrity of the share capital and guarantees creditors and third parties.

Apart from the cases of legal share capital reductions, In its typical form this offence occurs when the shareholders' contributions are returned to them, also by means of simulated transactions, or when shareholders are exempted from the obligation to make such contributions.

The offence envisages two possible conducts:

- Repayment of shareholder's contributions with reduction of the entire share capital fully paid in. The repayment may be clearly evident through a direct payment or simulated (partially or in full) through a payment against non-existing or lower-amount of services provided or through other behaviours corresponding to other offences (for example, a simulated profit distribution or interim dividend paid using the share capital).

- Exempting shareholders from the obligation to make the required share capital contribution.

Repayments relate to any shareholders' contribution (cash, credits, assets) required to set up those minimum assets needed to run the business.

- **Unlawful distribution of profits and reserves (art. 2627 of c.c.):**

"*Unless a major crime is committed, directors, who distribute profits or make advance payments on non existing profits or profits allocated by law to reserves, or repay non-distributable reserves, are punished with a prison sentence up to one year.*

The criminal liability is extinguished if profits or reserves are paid back before the deadline for approval of relevant financial statement".

The provision rules a specific offence of directors and aims to protect creditors from any "*impairment of their guarantees represented by share capital and other mandatory reserves*".

"*The repayment relates to the concrete wealth transfer from the company to other parties*".

Repayment may include profits or advance payments on non existing profits or profits allocated by law to reserves, or reserves that may not be distributed by law.

The offence is punished in case of negligence and fraud.

Paragraph 2 introduces a specific non-punishability clause if profits or reserves are paid back before the deadline for the approval of financial statement.

- **Unlawful dealing in stocks or shares of the company or parent company (art. 2628 of c.c.):**

"Unless permitted by laws, directors who purchase or subscribe stocks or shares in the company, causing damage to the integrity of the share capital or non-distributable reserves, are punished with a prison sentence up to one year.

Unless permitted by laws, the same sanction applies to directors who purchase or subscribe stocks or shares in the parent company, causing damage to the integrity of the share capital or non-distributable reserves.

The criminal liability is extinguished if the share capital or reserves are paid back before the deadline to approve the financial statement for the period when the offence was perpetrated".

Apart from the cases permitted by law, this offence is committed by purchasing or subscribing stocks or shares in the company or parent company, when such action damaged the integrity of the share capital or non-distributable reserves.

It should be noted that if the share capital or the reserves are restored before the deadline for approval of the financial statements for the period in which the event took place, then the offence is extinguished.

Directors are the only actors for this kind of offence.

- **Transactions prejudicial to creditors (art. 2629 of c.c.):**

"*Directors who, in breach of the provisions of the law protecting creditors, reduce share capital or merge with other companies or split the company and cause damage to the creditors, are punished, upon formal complaint of the offended party, with a prison sentence from six months to three years.*

Repayment of any damage caused to creditors before the sentence extinguishes the criminal liability".

The provision rules an offence committed by directors and aims to protect the share capital and guarantee the creditors' interest, following a transaction executed by the directors (e.g. share capital reduction, merger, split) with the purpose of eluding specific legal prescriptions.

The unlawful conducts include:

- Reduction of share capital not allowed by laws or below its minimum legal threshold;

- Merger with a distressed company which, in the event of insolvency procedure, may damage creditors of the healthy company (since they share guarantees with creditors of the distressed company);

- Company splits that may damage creditors.

Following the unlawful conduct by the directors, the damage materialises only when creditors ended up in a worse situation.

The provision envisages a generic fraudulence corresponding to the awareness and intention to specifically breach relevant regulations and procure damages to creditors.

Last paragraph introduces a non-punishable clause if damage is restored before the final sentence.

Finally, the offence may be punishable upon request of the offended party by formally filing a complaint.

- **Failure to disclose conflicts of interest (art. 2629-bis c.c.):**

"The director of a company with financial instruments listed on the Italian or other European markets or mainly sold to the generic public pursuant to art. 116 of D.Lgs. no. 58 of 24 February 1998 and subsequent amendments or subject to supervision pursuant to D.Lgs. no. 385 of 1 September 1993, of the previously mentioned D.Lgs. no. 58, D.Lgs. no. 209 of 7 September 2005 or D.Lgs. no. 124 of 21 April 1993, who breaches any of the duties listed on the first paragraph of art. 2391, is punished with a prison sentence from one to three years, when the company or third parties suffered damages, as direct consequence of his/her conducts".

The offence is perpetrated when the director of a listed company does not disclose his/her personal interest or someone else's interest, on a specific transaction.

The offence is extended also to the chief executive officer who does not refrain from the transaction when he/she is personally involved.

The offence relates to directors as well as to the chief executive officer.

- **Capitalising fictitiously (art. 2632 of c.c.):**

"*Directors and shareholders who make fictitious capital contributions or increase fictitiously the company's share capital by assigning a number of stocks or shares for an overall value exceeding the share capital, by mutual underwriting of stocks or shares, by substantially overvaluing contributions of assets receivables or by overvaluing the company's assets in the event of company transformation, are punished with prison sentence up to one year".*

The current provision aims to preserve the integrity of the share capital.

The offence is mainly related to directors and shareholders and applies to a generic fraudulent conduct.

Typical unlawful conducts include the following ones:

- Assigning shares or stocks for an overall value exceeding the share capital;
- Mutual underwriting of stocks or shares;
- Overvaluing contributions of assets or receivables or the company's assets.

On this purpose, it shall be noted that during the incorporation of a limited company or the increase of share capital (by contributing assets or receivables) as well as in the event of a company transformation from partnership to limited company, it is always required a valuation report pursuant to art. 2343 of c.c., with the exception ruled by art. 2343-ter of c.c.

The subject appointed for the valuation shall confirm that the contribution value is higher than the shares or stocks value or, in the event of a transformation, shall determine the precise value of the company's assets (under any circumstance, not lower to the minimum legal share capital).

Given that the subject is appointed by the Court and given that art. 2343 of c.c. does not envisage any consequence for directors not complying with their duties (as set in paragraph three of the same article) there is an open debate on whether or not directors shall be liable. On this purpose it is worth noticing that, according to common practice consolidated in the past, directors shall be liable pursuant to art. 40, par. 2 of C.P. However, recently such practice has been strongly criticised given that, pursuant to art. 2343 of c.c, the directors' obligation to control is subsequent to the offence.

- **Improper distribution of the company's assets by its liquidators (art. 2633 c.c.):**

"Liquidators who distribute the company's assets among the shareholders before paying off the company's creditors or before accumulating the amounts needed to match creditors' claims, thereby causing damage to the creditors, shall be punished, upon request of the offended party, with a prison sentence from six months to three years. The compensation for damages suffered before the final sentence shall extinguish the crime".

The offence is perpetrated when shareholders are refunded, also by means of simulation, with contributions, unless there is a legitimate reduction of share capital, or when shareholders are exempted from the obligation to make such contributions.

The provision related to directors. However, pursuant to art. 110 of C.P., there may be a criminal complicity by shareholders, who are recipients of the payment or the exemption, as long as they played a role in determining or influencing the unlawful conduct of directors.

- **Bribery among private individuals (art. 2635 c.c.):**

"Unless a major crime is committed, directors, general managers, director in charge of the accounting reports, statutory auditors and liquidators of companies or private entities who, directly or through other persons, solicit or receive undue money or other benefits or accept the promise thereof, in order to perform or omit an act contrary to their official duties or obligations of loyalty, are punished with a prison sentence from one to three years. The same sanction applies to those subjects who, within the company or private entity, hold a different managerial function from the one mentioned above.

Prison sentence up to one year and six months applies if the offence is perpetrated by an individual supervised by one of the subject identified in the first paragraph.

Any subject who, directly or through other persons, offers or promises undue money or other benefits to the subjects identified in the first and second paragraph, is punished accordingly.

Sanctions of previous paragraphs are doubled if the company issued financial instruments listed on Italian or other European markets or the instruments are mainly sold to the generic public pursuant to art. 116 of D.Lgs. no. 58 of 24 February 1998 and subsequent amendments.

The sanction is applied upon request of the offended person unless the offence affected the competitive process of purchasing goods and services.

Unless otherwise stated by art. 2641, the seizure shall be equal or higher the promise or benefits offered".

For the purpose of D.Lgs. no. 231/2001, it is considered only the case ruled by third paragraph of art. 2635 of c.c. where the offence relates to the bribe-giver procuring benefits to his/her company (active bribery). In particular, it relates to the unlawful conduct held by an individual who, directly or indirectly, offers or promises undue money or other benefits to directors, general managers, director in charge of the accounting reports, statutory auditors and liquidators as well as other individual supervised by these subjects, in order to perform or omit an act contrary to their official duties or obligations of loyalty. The D.Lgs. no. 38/2017 has therefore changed art. 2635 of c.c. by introducing the following news:

- Deletion of the wording «*damages to the company*» from par. 1 of art. 2635 of c.c. to assess whether or not the offence is committed; In this way, the timing of the offence is anticipated and the emphasis is put on the breach of official duties or obligation of loyalty by the bribe-taker;

- In addition to senior management, the inclusion of other persons holding managerial functions within the company or private entity; such inclusion is in line with the general principle of corporate offences set forth by art. 2639 of c.c., which includes also «de facto directors»;

- To punish also those subjects who, «*directly or through another person, offer or promise undue money or other benefits to the subjects identified in the first and second paragraph*»; this provision put emphasis on the conduct of the bribe-giver when relying of other persons to perpetrate the offence.

▪ **Instigating bribery among private individuals (art. 2635-bis of c.c.):**

"Any subject who offers or promises undue money or other benefits to directors, general managers, director in charge of the accounting reports, statutory auditors, liquidators and other individuals holding managerial functions in companies or private entities, in order to perform or omit an act contrary to their official duties or obligations of loyalty and the offering or promise is rejected, then the sanction in the first paragraph of art. 2635 is reduced by one third.

The sanction in the first paragraph applies to directors, general managers, director in charge of the accounting reports, statutory auditors, liquidators and other individuals holding managerial functions in companies or private entities who, directly or through another person, solicit money or other benefits or the promise thereof, in order to perform or omit an act contrary to their official duties or obligations of loyalty, and the offering or promise is rejected.

The sanction is applied upon request of the offended party".

D.Lgs. no. 38/2017 introduced the new offence "Instigating bribery among private individuals" as per art. 2635-bis of c.c. The legislator has therefore decided to sanction pure inducement to bribery among private individuals, also when there is a rejection of the offer or promise. For the purpose of the Decree, as per the offence of bribery among private individuals ruled by art. 2635 of c.c., it is considered only the active side of the bribery. In particular, it relates to the unlawful conduct held by an individual, who offers or promises undue money or other benefits to directors, general managers, director in charge of the accounting reports, statutory auditors and liquidators as well as other individual supervised by these subjects, in order to perform or omit an act contrary to their official duties or obligations of loyalty, and the offering or promise made is rejected.

- **Unlawfully influencing the shareholders' meeting (art. 2636 of c.c.):**

"Any subject who obtains, by simulation or fraud, a majority in the shareholders' meeting in order to achieve an unfair profit for himself/herself or for others, is punished with prison sentence from six months to three years".

The offence is therefore perpetrated in order to achieve an unfair profit (specific fraud) for himself/herself or for others and is implemented by simulation or fraud in order to reach the majority at shareholders' meeting.

For the purpose of the D.Lgs. no. 231/01, the offence shall be perpetrated by directors, general managers, liquidators or other individuals supervised by the aforementioned subjects.

- **Market rigging (art. 2637 of c.c.):**

"Any subject who spreads false information or simulates transactions likely to significantly alter the price of financial instruments not listed or for which no listing application on regulated markets is made, or likely to have a significant impact on public confidence in the financial stability of banks or banking groups, is punished with prison sentence from one to five years".

The offence is perpetrated when a subject, spreading false information or simulating transactions, alters significantly the price of financial instruments not listed or for which no listing application on regulated markets is made, or impacts significantly on public confidence in the financial stability of banks or banking group.

Offenders include also third parties of the company.

- **Obstruction of duties of the Public Supervisory Authorities (art. 2638 of c.c.):**

" Directors, general managers, director in charge of the accounting reports, statutory auditors, liquidators and other individuals subject to the supervision of public authorities who, when submitting mandatory communications to the public supervisory authorities, for the specific purpose of obstructing the Supervisory Authority's activity, disclose untrue material facts, although subject to further assessments, or conceal fraudulently specific facts that should have been reported concerning the economical and financial situation of company, are punished with prison sentence from one to four years. Offence is committed also in the event that information refers to assets held by the company on behalf of other parties.

The same sanction applies also to directors, general managers, director in charge of the accounting reports, statutory auditors, liquidators and other individuals subject to the supervision of public authorities, who take any measure specially to obstruct their activities, also omitting the submission of mandatory communication to public supervisory authorities,.

Sanction is doubled if the company issued financial instruments listed on Italian or other European markets or the instruments are mainly sold to the generic public pursuant to art. 116 of D.Lgs. no. 58 of 24 February 1998.

For the purpose of the criminal law, authorities and functions set forth by the decree implementing the EU directive 59/2014 are considered supervisory authorities and functions.

The offence is perpetrated when one of the following unlawful conducts apply:

- Disclosing to public supervisory authorities untrue facts on the economical and financial situation of the company;
- Concealing any fact to be disclosed;
- Obstructing, on purpose, activities of the public supervisory authorities;
- Concealing any fact to be disclosed to public supervisory authorities.

The actors of the offences include directors, general managers, statutory auditors and liquidators.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal;
- Occupational Health and Safety;
- Information Technology;
- Administration, finance and Internal Audit;
- Marketing and sales;
- Communication and promotions;
- Compliance/AML;
- Procurements of goods and services.

4. Sensitive activities related to corporate offences

From the analysis conducted by SNAITECH within each Division and Unit, the activities potentially exposed to perpetration of offences may be classified as follows:

- Activities exposed to "***direct risk of perpetrating the offence***";
- Activities that may "***contribute to perpetrating"*** a corporate offence. These activities are related to the management of financial instruments and therefore may be functional to generate black funds.

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to corporate offences, pursuant to articles 25-ter of the Decree:

- ✓ Management of the activities relating to the request for authorisation or fulfilment of requirements towards the public administration (e.g. NOE, CIV, POS building renovation permits, DIA, SCIA, etc.);
- ✓ Relations and activities with public officials and/or persons in charge of public service (e.g. ADM, GdF, AdE, MIPAAF, ASL, NAS, Technical offices of Municipalities, Labor inspectorate, INPS, INAIL, etc.), also through external advisors, during: inspections, controls and assessments;
- ✓ Selection and management of agents;
- ✓ Management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;
- ✓ Management of relations with clients/partners in the retail space (gaming machine owners, retailers, independent associations, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;
- ✓ Management of incentives paid to the distribution network (e.g. Additional compensation and bonus);
- ✓ Management and assessment of compliance with gambling parameters and proper functioning of gambling activities (compliance with ADM regulation);
- ✓ Management of terminals instalment and set up (roll-out and connectivity);
- ✓ Periodic inspections to verify compliance with concessions (AWP, VLT, ads);
- ✓ Warehouse inventory management;
- ✓ Management of the procedures for the procurement of goods and services (including screening of suppliers);
- ✓ Management of the procedures for the appointment of professional consultants (including screening and other relations (also of legal nature) with consultants);

- ✓ Management of direct and indirect taxation;
- ✓ Treasury activities including cash movements of bank accounts;
- ✓ Management and recording credit and debit invoices and receipts;
- ✓ Evaluation of company assets, recording and disclosing transactions in the ledger, reports, financial statements and other corporate documentation and budget plan as well as disclosing annual financial statements;
- ✓ Management of relations with Shareholders, Board of Statutory Auditors, independent auditor and storage of accounting documents (e.g. corporate documents, accounting records, general meeting minutes, etc.);
- ✓ Management of relations with financial institutions;
- ✓ Management of extraordinary corporate finance transactions (e.g. investment, bond issuance, transactions of financial instruments, investment or sale of shareholding in other undertakings, purchase or sale of undertakings or business units, mergers, splits, etc.);
- ✓ Screening, hiring and management of personnel (also indirectly through third parties);
- ✓ Management of corporate incentives and benefits;
- ✓ Management of business trips, advance payments and reimbursement of travel expenses
- ✓ Management of sponsorships and donations;
- ✓ Management of gifts;
- ✓ Management of entertainment expenses;
- ✓ Management of relations with judicial authorities during litigations (fiscal, administrative, civil, labour and appeals against the entity issuing the concession).
- ✓ Set up corporate strategies to manage litigations, including settlement agreements in judicial and non-judicial transactions (access to documentation, statements, interrogations and agreements);
- ✓ Management of intragroup relations (investments, contracts, information flows, etc.);
- ✓ Management of relations with related parties;
- ✓ Management of the AML procedure (risk profiling of customers, due diligence, storage and reporting to UIF, handling SOS and PEP, etc.).

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Specific prevention protocols

Transactions related to: **management of the activities relating to the request for authorisation or fulfilment of requirements towards the public administration (e.g. NOE, CIV, POS building renovation permits, DIA, SCIA, etc.); relations and activities with public officials and/or persons in charge of public service (e.g. ADM, GdF, AdE, MIPAAF, ASL, NAS, Technical offices of Municipalities, Labor inspectorate, INPS, INAIL, etc.), also through external advisors, during: inspections, controls and assessments; selection and management of agents; management of incentives paid to the distribution network (e.g. Additional compensation and bonus); management and assessment of compliance with gambling parameters and proper functioning of gambling activities (compliance with ADM regulation); management of terminals instalment and set up (roll-out and connectivity); periodic inspections to verify compliance with concessions (AWP, VLT, ads); management of the procedures for the procurement of goods and services (including screening of suppliers); management of the procedures for the appointment of professional consultants (including screening and other relations (also of legal nature) with consultants); management of direct and indirect taxation; treasury activities including cash movements of bank accounts; management and recording credit and debit invoices and receipts; screening, hiring and management of personnel (also indirectly through third parties); management of corporate incentives and benefits; management of business trips, advance payments and reimbursement of travel expenses; management of sponsorships and donations; management of gifts; management of entertainment expenses**. Provisions of par. 5 of Special Section A- Crimes against the public administration – apply in relation to sensitive activities.

Transactions related to: **management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement; management of relations with clients/partners in the retail space (gaming machine owners, retailers, independent associations, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement**. Protocols include the following steps:

- ✓ Roles and responsibilities of all subjects involved in the process are clearly identified;
- ✓ There is segregation of duties and responsibilities between subjects who authorise, execute and control the activities;
- ✓ The head of Sales shall select counterparties between more candidates and according to their expertise, reliability and availability;
- ✓ When selecting a counterparty outside the standard procedure, a specific authorisation by relevant Divisional Head is needed;
- ✓ The Company shall assess periodically the reliability and integrity of each counterparty;
- ✓ SB shall be informed of any relation, negotiation and or execution of acts/contracts with any subject included in the Reference Lists;
- ✓ ,Any draft of the contract shall be authorised by the legal office before third party submission;

- ✓ The Chief Executive Officer shall authorise in writing the execution of any contract with the selected parties;

- ✓ Contracts shall include specific clauses of compliance to ethical principle of the Company as well as rights to withdraw mandates in case of breaches; additionally third parties shall produce specific statements of non-conviction for one of the offences set forth by the D.Lgs. no. 231/01;

- ✓ Principles of the Ethical Code and Model must be acknowledged and accepted;

- ✓ When using a non-standard contractual template, clauses are drafted together with the legal office, which approves the draft to be submitted to the third party;

- ✓ It is forbidden to set compensation not in line with the services provided to the Company, the mandate, market practices or professional rates set for the relevant advisory activities;

- ✓ The person in charge of the relevant function shall store any documentation such that any further amendment is allowed only with specific authorisation and relevant evidence is provided (in order to ensure proper traceability of the process and facilitate any eventual subsequent control).

For transactions related to: **warehouse inventory management; evaluation of company assets, recording and disclosing transactions in the ledger, reports, financial statements and other corporate documentation and budget plan as well as disclosing annual financial statements**. Protocols include the following steps:

- ✓ Adopting accounting manual or procedures, which are constantly updated and clearly define data and information to be provided by each function and division, accounting criteria for data processing, timing and deadline to produce information, criteria to consolidate financial data from subsidiaries;

- ✓ Recording of business transactions shall comply with fairness, accuracy and completeness principles;

- ✓ Persons in charge of relevant corporate functions or subsidiaries shall promptly provide Administration and Finance Department with all the required information and state the completeness and accuracy of information (or eventually indicate those subjects who may release such statements);

- ✓ Persons in charge shall provide the original sources (or a copy) of the information to be produced, if relevant to understand information;

- ✓ Elaboration, transmission and aggregation of accounting data relevant for corporate disclosure shall be traceable in each step and clearly identify those subjects involved in the data entry; login credentials are clearly identified by the IT division which shall ensure the segregation of functions and coherence between authorisation levels;

- ✓ Any eventual change of accounting items or criteria shall be authorised by the Administration and Finance Department;

- ✓ Any unjustified request to change accounting criteria of elaboration, recording and disclosure or to amend recorded data shall be promptly reported to the Supervisory Body;

- ✓ Draft of financial statements and other documents shall be provided to directors well in advance of the board meeting scheduled to approve the financial statements;

- ✓ If the activities of current protocol are outsourced, then the Company shall notify the Ethical Code and Model to suppliers and shall impose contractual obligations to comply with their principles.

For transactions related to the **management of extraordinary corporate finance transactions (e.g. investment, bond issuance, transactions of financial instruments, investment or sale of shareholding in other undertakings, purchase or sale of undertakings or business units, mergers, splits, etc.)**. Protocols shall include the following steps:

- ✓ Transactions are approved by the Board of Directors of each undertaking involved in the transaction;

- ✓ The corporate function sponsoring the transaction or with relevant expertise, shall arrange any useful documentation to support the transaction along with a preliminary report describing contents, interests and strategic goals achievable;

- ✓ Independent auditor and the Board of Statutory Auditors shall formulate their opinion on the transaction, when required so;

- ✓ Administration and Finance department along with Legal and Corporate Affairs department shall assess, before bookkeeping the transaction, the completeness, relevance and fairness of any supporting documentation produced.

For transactions related to the **management of relations with Shareholders, Board of Statutory Auditors, independent auditor and storage of accounting documents (e.g. corporate documents, accounting records, general meeting minutes, etc.)**, protocols shall include the following steps:

- ✓ There is full cooperation and transparency when dealing with independent auditor, Board of Statutory Auditors and shareholders;

- ✓ Any request and transmission of data and information, communication and valuation made by shareholders and the Board of Statutory Auditors shall be registered and stored;

- ✓ Any document on transactions, which shall be discussed at general meeting, Board of Directors or submitted to the Board of Statutory Auditors for approval, shall be provided well in advance of the scheduled meetings;

- ✓ Board of Statutory Auditors and shareholders are granted with full access to the accounting system and any other information needed to perform their duties;

- ✓ Maintaining relations with independent auditor to obtain the relevant certification.

For transactions related to the **management of relations with financial institutions**, protocols shall include the following steps:

- ✓ There are specific procedures on roles, activities, responsibilities and controls related to the management of relations with financial institutions;
- ✓ Identify all relevant subjects authorised to manage relations with financial institutions;
- ✓ Relations with financial institutions and financial markets are handled with fairness and transparency, in full compliance with principles of proper management and information parity;
- ✓ Integrity, fairness and independency shall refrain from influencing other party's decisions or requesting more favourable conditions;
- ✓ All data and information disclosed to financial institutions shall be true, complete and accurate;
- ✓ It is clearly defined the traceability of management, disclosure and elaboration as well as access to privileged information;
- ✓ There is a clear procedure to elaborate, control and disclose corporate information, analysis, researches, strategic and business plans and other information relevant for the Company;
- ✓ There is full compliance with laws and regulations on relations with financial institutions and in particular when disclosing to supervisory authorities.

For transactions related to: **management of relations with judicial authorities during litigations (fiscal, administrative, civil, labour and appeals against the entity issuing the concession); set up corporate strategies to manage litigations, including settlement agreements in judicial and non-judicial transactions (access to documentation, statements, interrogations and agreements)**. Protocols include the following steps:

- ✓ There are clear procedures on roles, activities, responsibilities and controls required to manage litigations;
- ✓ Identify all relevant subjects authorised to act on behalf of the Company in litigations;
- ✓ All documents related to litigation shall be approved by the Chairman and Chief Executive Officer;
- ✓ Assess pro and cons of any potential action following the notification of a writ of summon;
- ✓ The legal advisor shall be selected according to the following criteria and principles: i) transparency; ii) equal opportunity; iii) professionalism; iv) reliability; v) inexpensiveness;
- ✓ Legal advisors are engaged on written contracts, which must be reviewed and authorised by the Chairman, Chief Executive Officer and Head of Legal and Corporate Affair;
- ✓ Management of the company shall be involved on developing litigation strategies;
- ✓ Management of the company is constantly updated on outstanding litigations;

- ✓ Any contractual relationship with legal advisors is formalised with a mandate letter;
- ✓ The mandate letter or contract shall include specific clauses on the acceptance of the Ethical Code and Model of SNAITECH;
- ✓ All the activities performed by the legal advisors shall be monitored through periodic reports to be stored;
- ✓ It is clearly defined the traceability of any person involved, any request of information received during the litigation and the process to assess and authorise disclosure of information;
- ✓ All documentation is stored by the person in charge of the relevant function in order to ensure traceability of the process and facilitate further controls.

For transactions related to: **management of intragroup relations (investments, contracts, information flows, etc.); management of relations with related parties**. Protocols shall include the following steps:

- ✓ Relations with group's undertakings shall be compliant with fairness and transparency principles. Relations with related parties shall be compliant with principles of autonomy, proper management, accounting transparency and segregation of assets, in order to protect stakeholders of all the undertakings;
- ✓ Management related party and intragroup transactions shall comply with roles, duties and responsibilities contained in the corporate structure and the authorisation system;
- ✓ Each group undertaking shall preserve its own autonomy and operational, managerial and financial independency;
- ✓ A related party register shall be arranged and updated, with the aim of tracking any transaction;
- ✓ The process of identifying counterparties involved on intragroup transactions shall be clearly defined;
- ✓ It is clearly identified the function responsible to set characteristics of intragroup transactions;
- ✓ Any related party transaction shall be classified according to specific criteria and on the basis of its its relevance and importance;
- ✓ There are clear procedures to manage and authorise related party transactions;
- ✓ There are specific disclosure duties during the execution of related party transactions;
- ✓ Any intragroup transaction shall be executed under written contracts;
- ✓ Qualified subjects shall assess the convenience of economic conditions applied to the intragroup transactions;
- ✓ Any document related to the transaction shall be stored.

For transactions related to the **management of the AML procedure (risk profiling of customers, due diligence, storage and reporting to UIF, handling SOS and PEP, etc.)**, the provisions of par. 4 of the Special Section E – Money laundering - apply in relation to sensitive activities.

6. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D. LGS. N. 231/01

Special Section C

Market Abuse
(Art. 25-sexies D.Lgs. n. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

The current Special Section refers to market abuse offences set forth by art. 25-sexies of D.Lgs. no. 231/2001, provides guidelines and conducts rules to prevent perpetration of offences ruled by D.Lgs. no. 231/2001 and ensure fairness and transparency of the business.

This sections defines specific rules to rightfullly implement the Model and provide the SB and other Control function with relevant tools to perform their monitoring, control and assessment activities.

2. Offences of art. 25-sexies of D.Lgs. no. 231/2001

2.1. Short notes on "Market rigging" offence set forth by art. 2637 of c.c. and covered by Special Section B – Corporate offences

Market rigging offence set forth by art. 2637 of c.c., included also in art. 25-ter of D.Lgs. no. 231/2001 on Corporate Offences, punishes the unlawful conduct of any subject who spreads false information or simulates transactions and alters significantly the price of financial instruments not listed or for which no listing application on regulated markets is made, or impacts significantly on public confidence in the financial stability of banks or banking group.

The specific offence covers only the financial instruments not listed with the aims to protect the market functioning.

2.2. Market abuse offences set forth by art. 25-sexies of D.Lgs. no. 231/2001

The current chapter covers the administrative offences related to market abuse.

In particular, art. 9, par. 3 of Law no. 62 of 18 April 2005 "*Measures for the implementation of obligations arising from Italy's membership of the European Communities – Community Law 2004*" enlarged the group of offences set forth by D.Lgs. no. 231/01, by including two additional crimes such as "Insider Trading" (art. 184 of D.Lgs. no. 58/1998) and "Market Manipulation" (art. 185 of D.Lgs. no. 58/1998), and ruled specific liabilities for the Company when these crimes are perpetrated in the interest or benefit of the Company.

In addition to the administrative liability for the market abuse offence, there is also an administrative liability for the "administrative offence". Although not included in the list of offences set forth by D.Lgs. no. 231/01, the provisions of art. 187-quinquies of D.Lgs. no. 58/1998 rule the "direct" administrative liability for the administrative offences connected to Insider Trading and Market Abuse, if perpetrated in the interest or benefit of the entity. The administrative offence differs from other crimes as it applies also in case of negligence of the offender (while no fraud is required).

Art. 187-quinquies rules also liability exemptions and places on the Entity the burden of proving that the perpetrator of the offence acted solely in his own or a third party's interest, pursuant to articles 6[1], 7[2], 8[3] e 12[4] of D.Lgs. no. 231/2001.

---

1. Art. 6, Senior Managers and organisational models, of D.Lgs. no. 231/2001, states the following:
"1. If the offence is committed by those individual listed in art. 5, par. 1, letter a) [Senior Managers], the entity shall not be liable if it may prove that: a) before the offence was committed, management adopted and effectively implemented organisational and management models aimed at preventing offences; b) the duties to supervise on functioning and compliance with models as well as ensuring constant update are attributed to an internal body with decision-making and control powers; c) individuals perpetrated the offence by fraudulently circumventing the models; d) there was no omission or insufficient controls by the internal body identified in letter b).
2. In relation to the extension of the delegated powers and to the risk of crimes being committed, the models as per letter a) of par. 1 shall satisfy the following requirements:
a. Identifying the activities within the context of which crimes might be committed;
b. Foreseeing specific protocols aimed to plan the elaboration and implementation of entity's decisions in relation to the crimes to be prevented;
c. Identifying ways of managing financial resources able to prevent the commission of crimes;
d. Foreseeing obligations of information for the body in charge of supervising the functioning and observance of the models;
e. Introducing a suitable disciplinary system to apply sanctions for the failure to respect the measures indicated in the model.
3. The models of organization and management may be adopted, guaranteeing the requirements as per par. 2, on the basis of the codes of conducts drawn up by the representative associations of the entities, communicated to the Ministry of Justice which, together with the competent Ministries, may formulate, within thirty days, observations on the suitability of the models to prevent crimes.
4. In small entities, the duties in letter b) par. 1 may be carried out by the relevant management body.
4-bis. In listed companies, the statutory auditors, the supervisory committee and risk committee may substitute the functions of the supervisory body indicated on par. 1, lett. b) (2).
5. It is in any case obligatory to confiscate the profit that the entity obtained from the crime, also in an equivalent form".

2. Art. 7, Persons subject to supervision by others and organisational models of the entity, of D.Lgs. no. 231/2001 states the following:
"1. In accordance with art. 5, par. 1, letter b) [Employees reporting to Senior Managers], the entity is deemed liable if the offence was perpetrated because of the non compliance with management and control duties.
2. In any case, non-observance of the obligations of management or supervision is excluded if the agency, prior to the commission of the crime, has adopted and effectively implemented a model of organization, management and control suitable to prevent crimes of the same sort as the one committed.
3. The model foresees, in relation to the nature and size of the organization and to the type of activity carried out, measures suitable to guarantee the carrying on of the activity in respect of the law and to discover and eliminate promptly any situations of risk.
4. The effective implementation of the model requires:
a. Periodic check and the possible modification thereof when any significant breaches of the prescriptions are discovered or when changes occur in the organization or activity;
b. A disciplinary system able to punish any failure to respect the measures indicated in the model".

3. Art. 8, Autonomy of entity's liabilities, D.Lgs. no. 231/2001 states the following:
"1. The entity is liable also in the following circumstances:
a. The offender has not been identified or is not chargeable;
b. The crime is extinguished for a cause other than amnesty.
2. Unless the law provides otherwise, action shall not be taken against the entity when an amnesty is granted for a crime and related liability and the offended party waived its application
3. Entity may waive the amnesty".

4. Art. 12, Scenarios for sanctions reduction, of D.Lgs. n. 231/2001, states the following:
"1. Monetary sanction is halved and may not be set above Euro 103,291.00 when: a) the offender acted in its own or third-party interest and the entity had minimum benefit if none; b) The entity of monetary damage is irrelevant.
2. Monetary sanction is reduced to one third when, ahead of the first-degree hearing: a) the entity has fully indemnified any damage and removed any negative consequences or acted with this intention; b) the entity adopted and implemented an organisational model aimed at preventing offences similar to the one committed.
3. When both conditions specified in previous paragraphs apply, the sanction is reduced from half to two thirds.
4. Under no circumstances the monetary sanction may be lower than 10,329".

On 3 July 2016, the EU Regulation no. 596/2014 ("Market Abuse Regulation" or "MAR") was implemented with the aim of:

- Establishes a common regulatory framework on insider dealing, the unlawful disclosure of inside information and market manipulation;
- Update and enhance the current framework by including new markets and trading strategies, new requirements to prevent market abuse with the aim of ensuring the integrity of European financial markets and enhancing investor protection and confidence in those markets;
- Enlarge the number of conducts relevant for market abuse including also the simple attempt.

MAR is a legally binding European act for all its recipients and aims to introduce a level playing field regulation on market abuse. MAR is applicable by each State member: recipients shall apply MAR in full. Any partial, incomplete or delayed implementation is illegitimate.

MAR introduced specific provisions for the above-mentioned offences (art. 184 and 185 of D.Lgs. no. 58/1998):

- Insider trading (art. 8 of MAR);
- Market manipulation (art. 12 of MAR).

The EU Regulation no. 596/2014 updated some of the definitions of the above-mentioned offences, as specified below.

For the purpose of the MAR Regulation, administrative offences relevant for the current Special Sections relates to:

- Financial instruments admitted to trading on a regulated market or for which a request for admission to trading on a regulated market has been made;
- Financial instruments traded on an MTF, admitted to trading on an MTF or for which a request for admission to trading on an MTF has been made;
- Financial instruments traded on an OTF[5];
- Financial instruments not covered by point (a), (b) or (c), the price or value of which depends on or has an effect on the price or value of a financial instrument referred to in those points, including, but not limited to, credit default swaps and contracts for difference;
- Transactions, including bids, relating to the auctioning on an auction platform authorised as a regulated market of emission allowances or other auctioned products based thereon, including when auctioned products are not financial instruments.

---

5. Art. 4, par. 1, point 23, (UE) Directive no. 65/2014, states that an organised trading facility means "*multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract in accordance with Title II of this Directive*".

Definition of privileged information is ruled by art. 181 of D.Lgs no. 58/1998 and is equally reported in art. 7[6] of MAR.

On 13 October 2017 Cosob issued two guidelines "Inside Information Guidelines no. 1/2017" and "Investment Recommendation Guidelines no. 2/2017") with the aim to clarify the EU regulation no. 596/2014 on market abuse and subsequent implementation acts. These guidelines shall be considered a supporting document to better understand duties arising from the European and national regulation.

The Inside Information Guidelines set out a non-binding process useful to carry-out a full self-assessment of the information that could become inside information and to manage the inside information, including the list of persons who have access to inside information ("Insider List"). In particular, Consob provides detailed indications to define internal procedures to identify and promptly report to relevant subjects any information that may become inside information (to be disclosed to the public).

Consob described how to identify, map and classify inside information, which shall refer only to any information and/or news deemed to be relevant for the issuer. It may include any data, event, project or circumstance which, continuously, repetitively, periodically or occasionally is directly related to the issuer and may, at a later stage, become privileged information. On this purpose, the Consob guidelines require the issuers to monitor any preliminary stage of disclosure.

The Inside Information Guidelines no. 1/2017 introduced important tools for the issuers of financial instruments to support their duties under art. 17, par. 4 of EU Regulation no. 596/2014. In particular, an issuer or an emission allowance market participant, may, on its own responsibility, delay the disclosure of inside information to the public provided that all of the following conditions are met:

- Immediate disclosure is likely to prejudice the legitimate interests of the issuer or emission allowance market participant;
- Delay of disclosure is not likely to mislead the public;
- The issuer is able to ensure the confidentiality of that information.

---

6. Inside information is defined by art. 181 of D.Lgs. no. 58/1998 "*For the purposes of this title inside information shall mean information of a precise nature which has not been made public relating, directly or indirectly, to one or more issuers of financial instruments or one or more financial instruments and which, if it were made public would be likely to have a significant effect on the prices of those financial instruments. In relation to derivatives on commodities, inside information shall mean information of a precise nature which has not been made public relating, directly or indirectly, to one or more such derivatives and which users of markets on which such derivatives are traded expect to receive in accordance with accepted market practices on those markets.*
Information shall be deemed to be of a precise nature if:
a) It refers to a set of circumstances which exists or may reasonably be expected to come into existence or an event which has occurred or may reasonably be expected to occur; and
b) It is specific enough to enable a conclusion to be drawn as to the possible effect of the set of circumstances or event referred to in paragraph a) on the prices of financial instruments.
Information which, if made public, would be likely to have a significant effect on the prices of financial instruments shall mean information a reasonable investor would be likely to use as part of the basis of his investment decisions.
For persons charged with the execution of orders concerning financial instruments, inside information shall also mean information conveyed by a client and related to the client's pending orders, which is of a precise nature, which relates directly or indirectly to one or more issuers of financial instruments or to one or more financial instruments and which, if made public, would be likely to have a significant effect on the prices of those financial instruments".

The same articles furthermore envisage that, if an issuer or emission allowance market participant has delayed the disclosure of inside information under this paragraph, it shall inform the competent authority that disclosure of the information was delayed and shall provide a written explanation of how the conditions set out in the paragraph were met. This latter circumstance is specifically addressed by the Inside Information Guidelines no. 1/2017 (par. 6.8.2), which acknowledges ESMA view contained in document "*Questions and Answers on the Market Abuse Regulation* (*MAR*) – *Version 8*", issued on in 29 September 2017. In particular, where the issuer has delayed the disclosure of inside information and the information subsequently loses the element of price sensitivity, the issuer is not obliged to inform the competent authority that disclosure of such information was delayed.

Investment Recommendation Guideline no. 2/2017 provides indication on obligation and duties to present and disclose investment recommendation, disclose interests or indicate conflict of interests of individuals who produce and/or disclose investment recommendations. In particular, the guideline relates to those persons producing or disseminating investment recommendations, recipients of investment recommendations, issuers subject of investment recommendations and journalists disseminating information related to investment recommendations.

Art. 25-*sexies* of D.Lgs. n. 231/2001 includes the following offences:

- Art. 184 of D.Lgs. no. 58/1998 (Insider trading) – equally reported in articles 8 (Insider Trading) and 10 (Unlawful disclosure of inside information) of MAR
- Art. 185 of D.Lgs. no. 58/1998 (Market manipulation) – equally reported in art. 12 of MAR
- Administrative offences under art 187-quinquies of D.Lgs. no. 58/1998
- Art. 181 of D.Lgs. no. 58/1998 (Inside information) – equally reported in art. 7 of MAR

Art. 184[7] of D.Lgs. no. 58/1998 (Insider trading) – equally reported in articles 8 (Insider Trading) and 10 (Unlawful disclosure of inside information) of MAR

The offence is perpetrated where any person who, possessing inside information by virtue of his membership of the administrative, management or supervisory bodies of an issuer, his holding in the capital of an issuer or the exercise of his employment, profession, duties, including public duties, or position:

a. Buys, sells or carries out other transactions involving, directly or indirectly, for his own account or for the account of a third party, financial instruments using such information;
b. Changes or withdraws orders on financial instruments related to the information after having obtained inside information.

It is also considered insider trading the conduct of changing or withdrawing orders on financial instruments related to the information before having obtained inside information.

In relation to auctioning of greenhouse gas emission and other related assets pursuant to EU Regulation n. 1031/2010, insider trading is perpetrated also when a person presents, amends or withdraws offers for his own account of for the account of a third party.

The offence is perpetrated when a person, in possess of inside information, discloses such information to other parties outside the normal exercise of his employment, profession, duties.

---

7. Art. 184 of D.Lgs. n. 58/1998 states the following "*Imprisonment for between one and six years and a fine of between twenty thousand and three million euro shall be imposed on any person who, possessing inside information by virtue of his membership of the administrative, management or supervisory bodies of an issuer, his holding in the capital of an issuer or the exercise of his employment, profession, duties, including public duties, or position:*

a. Buys, sells or carries out other transactions involving, directly or indirectly, for his own account or for the account of a third party, financial instruments using such information;
b. Discloses such information to others outside the normal exercise of his employment, profession, duties or position;
c. Recommends or induces others, on the basis of such information, to carry out any of the transactions referred to in par. a).

The punishment referred to in paragraph 1 shall apply to any person who, possessing inside information by virtue of the preparation or execution of criminal activities, carries out any of the actions referred to in paragraph 1.
Courts may increase the fine up to three times or up to the larger amount of ten times the product of the crime or the profit therefrom when, in view of the particular seriousness of the offence, the personal situation of the guilty party or the magnitude of the product of the crime or the profit therefrom, the fine appears inadequate even if the maximum is applied.
With regard to financial instrument transactions pursuant to Article 180, paragraph 1, paragraph a), point 2), the judicial sanction shall involve infliction of a fine of up to one hundred and three thousand two hundred and ninety-one euro and up to three-years' imprisonment.
For the purposes of this article, financial instruments shall also mean financial instruments referred to in Article 1(2) whose value depends on a financial instrument referred to in Article 180(1)(a)".

The offence set forth by art. 184 of D.Lgs no. 58/1998, also know as "Insider trading" aims to preserve transparency and market functioning by improper use of privileged information. The point was already addressed by the jurisprudence, which acknowledged that the higher level of information obtained without any analysis and research creates disparity and discourages investors.
The offence may be perpetrated only by the individuals identified from the regulator:
• Members of the administrative, management or supervisory bodies of the issuer ("corporate insiders");
• Shareholders of an issuer ("shareholders insiders");
• Exercising activities, profession, duties, also public duties, or positions ("temporary insiders" such has legal advisors of the issuer or individuals holding positions in other public or private entities).
The latter category enlarges significantly the list of possible offenders and shall include also, pursuant to par. 2, any person who, possessing inside information by virtue of the preparation or execution of criminal activities, carries out any of the actions referred to in paragraph 1 ("criminal insiders").
It must be highlighted the emphasis put on the causality between role performed and information obtained. On this purpose, it is not sufficient to hold certain positions to be considered an insider, instead the position shall be used to obtain inside information.

Art. 185[8] of D.Lgs. no. 58/1998 (Market manipulation) – equally reported in art. 12 of MAR

The offence is perpetrated where a person manipulates market by:

- Entering into a transaction, placing an order to trade or any other behaviour which:
  - Gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances; or
  - Secures, or is likely to secure, the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances at an abnormal or artificial level;

- Unless the person entering into a transaction, placing an order to trade or engaging in any other behaviour establishes that such transaction, order or behaviour have been carried out for legitimate reasons, and conform with an accepted market practice;

---

8. Art. 185 of D.Lgs. no. 58/1998 states that: "*Imprisonment for between one and six years and a fine of between twenty thousand and three million euro shall be imposed on any person who disseminates false information or sets up sham transactions or employs other devices concretely likely to produce a significant alteration in the price of financial instruments.*
Courts may increase the fine up to three times or up to the larger amount of ten times the product of the crime or the profit therefrom when, in view of the particular seriousness of the offence, the personal situation of the guilty party or the magnitude of the product of the crime or the profit therefrom, the fine appears inadequate even if the maximum is applied.
With regard to financial instrument transactions pursuant to Article 180, paragraph 1, paragraph a), point 2), the judicial sanction shall involve infliction of a fine of up to one hundred and three thousand two hundred and ninety-one euro and up to three-years' imprisonment".
The offence of market manipulation included now several offences – on financial instruments of art. 180 of D.Lgs. no. 58/1998 – previously included in the offence of market rigging, pursuant to art. 2637 of c.c.
On this purpose art. 9, par. 4 of European Law 2004 states that: "in art. 2737 of civil code the wording <<financial instruments listed and not listed>> is replaced with <<financial instruments not listed or for which no listing application on regulated markets is made>>".
Therefore, art. 185 of D.Lgs. no. 58/98 identifies a common offence.
However it is clear that, pursuant to D.Lgs. no. 231/01, the crimes identified by the regulator may be perpetrated easily:
- On one side by corporate representative authorised to put in place such transactions;
- On the other side, individuals in charge of disseminating information. On this purpose, it shall be noted that the administrative offence ruled by art. 187-ter of D.Lgs. no. 58/98, provides specific indication on information activities conducted by journalists.

As mentioned, the offence is perpetrated through different and alternative conducts:
- Dissemination of false information;
- Setting up sham transactions;
- Employs other devices concretely likely to produce a significant alteration in the price of financial instruments.

In relation to "other devices", the legal common understanding clarified that market manipulation may be perpetrated with real transactions, seemingly legal and with a economic risk profile, which combined or implemented in a specific time and venue, may intentionally produce a significant alteration in the price of financial instruments – such that investors may be induced to have a different perception of the real market trend.
The alteration of market must be assessed ex post, based on the actual circumstances or on the effective market situation at the time of the manipulation.
In particular, the alteration in the price, relevant for the perpetration of the offence, shall be observed by analysis the difference between last price after market manipulation and last price without market manipulation.
The sanctions applicable in case of market manipulation are similar to the ones applied for insider trading, with the exception of the maximum threshold of the administrative fine set forth by art.185 of D.Lgs. no. 58/1998.

- Disseminating information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances or secures, or is likely to secure, the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances at an abnormal or artificial level, including the dissemination of rumours, where the person who made the dissemination knew, or ought to have known, that the information was false or misleading;

- Transmitting false or misleading information or providing false or misleading inputs in relation to a benchmark where the person who made the transmission or provided the input knew or ought to have known that it was false or misleading, or any other behaviour which manipulates the calculation of a benchmark;

The following behaviour shall, inter alia, be considered as market manipulation:

- The conduct by a person, or persons acting in collaboration, to secure a dominant position over the supply of or demand for a financial instrument, related spot commodity contracts or auctioned products based on emission allowances which has, or is likely to have, the effect of fixing, directly or indirectly, purchase or sale prices or creates, or is likely to create, other unfair trading conditions;

- Buying or selling of financial instruments, at the opening or closing of the market, which has or is likely to have the effect of misleading investors acting on the basis of the prices displayed, including the opening or closing prices;

- Placing of orders to a trading venue, including any cancellation or modification thereof, by any available means of trading, including by electronic means, such as algorithmic and high-frequency trading strategies, and which has one of the effects referred to in paragraph 1(a) or (b), by:

  i. Disrupting or delaying the functioning of the trading system of the trading venue or being likely to do so;

  ii. Making it more difficult for other persons to identify genuine orders on the trading system of the trading venue or being likely to do so, including by entering orders which result in the overloading or destabilisation of the order book; or

  iii. Creating or being likely to create a false or misleading signal about the supply of, or demand for, or price of, a financial instrument, in particular by entering orders to initiate or exacerbate a trend.

- Taking advantage of occasional or regular access to the traditional or electronic media by voicing an opinion about a financial instrument, related spot commodity contract or an auctioned product based on emission allowances (or indirectly about its issuer) while having previously taken positions on that financial instrument, a related spot commodity contract or an auctioned product based on emission allowances and profiting subsequently from the impact of the opinions voiced on the price of that instrument, related spot commodity contract or an auctioned product based on emission allowances, without having simultaneously disclosed that conflict of interest to the public in a proper and effective way;

- Buying or selling on the secondary market of emission allowances or related derivatives prior to the auction held pursuant to Regulation (EU) No 1031/2010 with the effect of fixing the auction clearing price for the auctioned products at an abnormal or artificial level or misleading bidders bidding in the auctions (see art. 12 of MAR).

Administrative offences under art 187-quinquies of D.Lgs. no. 58/1998

Entities shall be liable for administrative sanction imposed for offences committed in their interest or to their advantage:

a. by persons performing representative, administrative or management functions in the entity or one of its organisational units having financial and functional autonomy and by persons who, de facto or otherwise, manage and control the entity;
b. Persons subject to the direction or supervision of a person referred to in paragraph a).

Art. 181 of D.Lgs. no. 58/1998 (Inside information) – equally reported in art. 7 of MAR

For the purposes of art. 7 of MAR, inside information means a specific and non public information, directly or indirectly related to one or more issuers of financial instruments or one or more financial instruments and which, if made public, would be likely to have a significant effect on the prices of the financial instruments.

Information shall be considered specific where it indicates a set of circumstances which exists or which may reasonably be expected to come into existence, or an event which has occurred or which may reasonably be expected to occur, where it is specific enough to enable a conclusion to be drawn as to the possible effect of that set of circumstances or event on the prices of the financial instruments or the related derivative financial instrument, the related spot commodity contracts, or the auctioned products based on the emission allowances.

In this respect in the case of a protracted process that is intended to bring about, or that results in, particular circumstances or a particular event, those future circumstances or that future event, and also the intermediate steps of that process which are connected with bringing about or resulting in those future circumstances or that future event, may be deemed to be precise information.

An intermediate step in a protracted process shall be deemed to be inside information if, by itself, it satisfies the criteria of inside information as referred to in this Article.

Information which, if it were made public, would be likely to have a significant effect on the prices of financial instruments, derivative financial instruments, related spot commodity contracts, or auctioned products based on emission allowances shall mean information a reasonable investor would be likely to use as part of the basis of his or her investment decisions.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Administration, finance and Internal Audit;
- Information Technology;
- Business;
- Communication and promotions;
- Compliance;
- Legal.

4. Sensitive activities related to market abuse offences

Art. 6, par. 2, lett. a) of D.Lgs. no. 231/01 highlights the identification of Sensitive Activities as a key element of the organisational, management and control model. Given the specific nature of the business run by SNAITECH, the following Sensitive Activities were identified in relation to market abuse offences:

- ✓ Disclosure of mandatory information pursuant to D.Lgs. 58/07 and Issuers' Regulation (corporate releases and privileged information);
- ✓ Evaluation of company assets, recording and disclosing transactions in the ledger, reports, financial statements and other corporate documentation and budget plan as well as disclosing annual financial statements;
- ✓ Management of relations with investors and financial intermediaries;
- ✓ Management of extraordinary corporate finance transactions (e.g. investment, bond issuance, transactions of financial instruments, investment or sale of shareholding in other undertakings, purchase or sale of undertakings or business units, mergers, splits, etc.);
- ✓ External communication and management of relations with mass media (institutional as well as products/service/events communication).

As an example only, inside information may include:

- ✓ Entrance or leaving business segments;
- ✓ Resignation or appointment of member of corporate governance bodies or supervisory body;
- ✓ Renunciation of the mandate by the independent auditor;
- ✓ Purchase or sales of shareholdings, other assets or business units;
- ✓ Transactions on share capital;
- ✓ Issuance of warrants, financial instruments, bonds and other debt instruments;
- ✓ Amendments to the rights of financial instruments;
- ✓ Relevant losses potentially affecting net assets value;
- ✓ Merger and split transactions;
- ✓ Execution, amendment or termination of relevant contracts or agreements;
- ✓ Completion of procedures related to intangibles such as licences, patents, inventions;
- ✓ Crisis management situations;
- ✓ Litigations;
- ✓ Change of individuals holding strategic roles within the Company;
- ✓ Transactions on treasury shares;
- ✓ Instances or notification of insolvency procedure;
- ✓ Request for insolvency procedure;
- ✓ Related party transactions (as per Consob regulation no. 17221 of 12 March 2010);
- ✓ Release by the auditing company of qualified opinion, adverse opinion or disclaimer of opinion;
- ✓ Accounting information to be disclosed in the financial statements, consolidated financial statements and semi-annual financial statement as well as other information to be disclosed in the interim reports, when this information is disclosed to third parties, unless these parties are authorised by law and comply with confidentiality duties;
- ✓ Resolutions of the Board of Directors approving draft of financial statement, allocation of net profits, dividend distribution, consolidated financial statement, semi annual financial statement and interim reports.

The Board of Directors may produce any further addition to the above Sensitive Activities.

5. Prevention protocols and controls system

The Company acknowledged contents of EU Regulation no. 596/14, D.Lgs. no. 58/1998, Consob regulation, SNAITECH Corporate Governance system, principles of Ethical Code, Internal Dealing regulation and procedure "Management of corporate and inside information on SNAITECH".

The controls system implemented by the Company in relation to Sensitive Activities include:

- General prevention protocols (described in par. 2 of the Introduction to Special Sections);
- Specific prevention protocols related to the aforementioned Sensitive Activities and detailed in the following pages.

6. Specific prevention protocols

Recipients of the current Special Section, when performing their offices, shall acknowledge and comply with the following:

- Italian and foreign laws applicable to sensitive activities;
- Provisions of the Model;
- Ethical Code;
- Procedures and guidelines of SNAITECH including any documentation on the organisational, management and control Model of the Company.

For transactions related to: **disclosure of mandatory information pursuant to D.Lgs. 58/07 and Issuers' Regulation (corporate releases and privileged information); external communication and management of relations with mass media (institutional as well as products/service/events communication)**. Protocols include the following steps:

- When a relevant information[9] is originated and subsequently classified as inside information, then it shall be immediately disclosed[10] to the public according to the procedure implemented by the Company and current law;
- Inside information shall be disclosed through the storage systems (SDIR) and (SSA) authorised by Consob. The same information shall be published on the Company website, IR section, and shall be stored for at least 5 years from the publication date;

---

9. Relevant information is any information, which may become inside information although currently it does not fulfil all the requirements.

10. Upon certain conditions and requirements, the Company may decide to postpone the disclosure of inside information (see. Inside information procedure and inside register procedure).

- The issuer shall take care of the website by implementing, among other things, also the following procedures:
  - Disclose data and news on the website according to editorial criteria which aim to properly inform investors and avoid any promotional activity;
  - Disclose on each page of the website, date and time of the update;
  - In case of wrong information on the website, a corrigendum shall be disclosed immediately;
  - Full documents shall be made available to the public. If a summary is provided then it should fully reflect the key information of the original document;
  - Specify whether a full or partial version of documents is published on the website. If a partial version is published, then the indication to access full version shall be provided.

In relation to the aforementioned Sensitive Activities, SNAITECH identified the following:

- Duties and roles of persons in charge of managing inside information;
- Rules and procedures to follow when handing and disseminating inside information;
- Criteria to classify inside information according to the opinion of relevant functions and SB;
- Measures to protect, store and update information and to avoid unauthorised disclosure;
- Persons with access to relevant or inside information, given their activities or offices performed;
- Arrangement of an inside register to record any person with access to relevant or inside information, given their activities or offices performed. In particular, criteria to access and update the register shall be clearly set in advance. The inclusion in the inside register shall be promptly notified to the interest party as to comply with relevant procedures and prohibitions.

Any time there is a transaction involving inside information, all persons involved shall be included in the inside register. In particular, the register shall include any person with regular or occasional access to inside information or other persons with access to inside information, on the basis of his/her activities and duties performed.

Recipients shall refrain from:

- Acting, collaborating or behave, directly or indirectly, such that one of the offence of art. 25-sexies of D.Lgs. no. 231/01 may be perpetrated;
- Buying, selling or carrying out other transactions involving, directly or indirectly, for his own account or for the account of a third party, financial instruments using such information;
- Disclosing or disseminating false information with the intention to alter significantly the price of financial instruments;
- Setting up sham transactions or employs other devices concretely likely to produce a significant alteration in the price of financial instruments

For transactions related to: **evaluation of company assets, recording and disclosing transactions in the ledger, reports, financial statements and other corporate documentation and budget plan as well as disclosing annual financial statements; management of relations with investors and financial intermediaries**. Protocols specifically rule the circumstance of a voluntary disclosure of business forecasts (forecast and targets). The Company, in this case, shall arrange a press release by providing details on the forecasts and whether they refers to budget or strategic goals.

For transactions related to **management of extraordinary corporate finance transactions (e.g. investment, bond issuance, transactions of financial instruments, investment or sale of shareholding in other undertakings, purchase or sale of undertakings or business units, mergers, splits, etc.)**, protocols require extra care on transmission of documents related to the transactions and the exchange of information and/or documentation with consultants or legal advisors of the Company or Recipients.

7. Additional procedural principles

A non-exhaustive list of general conduct rules for Recipients is the following:

- The Company takes extra care of the transmission of any relevant document to members of Board of Directors and Statutory Auditors. On this purpose, the tool used to transmit documents shall ensure confidentiality.

- Same care shall be used, in extraordinary transactions, when exchanging information and/or documentation with consultants and legal advisors of the Company or Recipients;

- Any paper based document on confidential, relevant or inside information shall be stored and locked; documents may be used only for the time needed while unused documents shall be stored again; documents may be left on desk only for the time needed, especially when unauthorised subjects may have access to them;

- The same rules apply on business trips. In particular, documents shall never be left unattended;

- Implement specific measures to ensure confidentiality when opening or distributing mails with post office or couriers;

- Each paper-based or digital document shall report the wording “confidential” and may circulate only using selected folders.

Furthermore, the Company shall set an information-training program (for the Recipients) on market abuse offences and related corporate procedures.

8. Information flows to the SB

Persons in charge of relevant functions shall report periodically any information to the SB in accordance with protocols and procedure “Management of the information flows to the SB”.

In addition to the duties and functions of the SB listed on the General Section of the Model, the SB shall specifically perform the following activities in relation to the market abuse prevention:

- Verify compliance, implementation and adequacy of the Model to prevent market abuse offences set forth by the Decree;
- Supervise on the effective implementation of the Model and report any unusual behaviour noticed when analysing information flows and reports received;
- Assess periodically, also with the help of relevant functions, proxies and authorisations;
- Inform relevant bodies of any breach of the Model in order to apply sanctions;
- Constantly update the Model by proposing any relevant measure to preserve effectiveness and/or adequacy of the Model.

The SB runs autonomously specific controls on activities related to market abuse with the aim of assessing their compliance with the Model. On this purpose the SB is granted with full access to all relevant documentation.

The SB informs the Board of Directors and the Statutory Auditors on the outcome of its supervisory activity.

9. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

D.LGS. N. 231/2001

Special Section D

INVOLUNTARY MANSLAUGHTER OR INVOLUNTARY GRIEVOUS BODILY HARM PERPETRATED AGAINST OCCUPATIONAL SAFETY AND HEALTH LAW

(Art. 25 *septies* D.Lgs. n. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

The current Special Section refers to the offences set forth by art. 25-septies of D.Lgs. no. 231/2001 (**Occupational Safety and Health**) and aims to: identify prohibitions, set specific protocols to control all subjects involved in Sensitive activities listed below, prevent perpetration of the following crimes and ensure fairness and transparency of the business, in accordance with art. 30 od D.Lgs. 81/2008.

2. Offences fo art. 25 *septies* del D.Lgs. n. 231/2001

The following offences, ruled by art. 25-septies of D.Lgs. 231/01, may be potentially applicable to the company business:

- **Involuntary manslaughter (art. 589 of C.P.);**
- **Involuntary serious or grievous bodily harm (art. 590 of C.P.).**

Articles 589 and 590, par. 3, of C.P. recalled by art. 25-septies of Decree punish a person who unintentional kills (manslaughter) or unintentionally causes serious or grievous bodily injury.

Serious bodily injury indicates a condition which endangers the life of the injured person, or causes incapacity to attend to normal activities for a period exceeding forty days, or an injury which results in the permanent weakening of a sense or an organ; grievous bodily injury indicates a probably incurable condition; the loss of a sense, a limb, an organ or the capacity to procreate, permanent impairment of the power of speech, and facial deformity or permanent disfigurement

The offence, which may be a serious or grievous injury or death, may be perpetrated by an active conduct (the offender damages the integrity of another person) or omission (the offender does not intervene to prevent the offence he/she was supposed to prevent). A subject is liable of an omission when his/her conduct harms the integrity or life of a person whom the offender is obliged to prevent, in accordance with a contract. The legislator sees the employer as the guarantor of the "physical integrity and moral personality of employees" and its position of guarantor may be transferred as long as there is a specific written proxy, which includes all the authoritative and decision-making powers relevant to grant safety of employees. The person in charge shall be competent and experienced on the topic related to the transfer. Therefore, the active conduct is held by the person who materially causes the offence, while the omission is typical of the subject who is not compliant with his/her surveillance and control duties (e.g. employer, manager, etc.) and therefore does not intervene to prevent the offence.

For the administrative liability, manslaughter or bodily hams shall result from negligence: the unlawful conduct may be generic (breach of consolidated rules of social conducts) or specific (breach of specific laws, regulations, orders or disciplines). This differs remarkably from other offences set forth by the Decree, which result instead from voluntary intention.

Pursuant to D.Lgs. no. 231/01, the unlawful conduct of the offender perpetrating manslaughter or serious or grievous bodily harms shall result from violation of occupational safety and health regulations. In relation to the implementation of the Model, it should be noted that:

- ✓ Compliance with minimum safety standards imposed by sectorial regulation does not exempt from the overall diligence level requested;
- ✓ Application of safety standards to minimise (or remove, where possible) any risk of injury or illness, by relying to best-known techniques and science as well.
- ✓ There is a partial waiver of liability only when the injured employee did not take all the necessary precautions, which otherwise would have neutralised the underlying risk. There is a full waiver of liability in those circumstances characterised by exceptional, abnormal, exorbitant behaviour of the employee in relation to the work, input received or common safety.

Regulation on accident prevention covers employees and any individual, who legitimately entered the company's premises.

The list of subjects who may potentially perpetrate these offences may include:

- ✓ Employee, who may endanger his/her or someone else's safety and health;
- ✓ Manger and person in charge, who may also be responsible of coordination, supervision and training;
- ✓ Employer as the key actor in preventing and protecting;
- ✓ Designer, who shall comply with prevention principles on occupational safety and health when taking his/her planning and technical decisions;
- ✓ Manufacturer, installer and maintenance technician who shall ensure compliance with relevant regulations when performing their offices;
- ✓ Contractor.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal
- Occupational safety and health;
- Compliance;
- Procurement of goods and services
- HR.

4. Sensitive activities related to occupational safety and health offences

4.1. General considerations

A preliminary identification of sensitive activities, pursuant to D.Lgs. no. 231/2001, focuses on those activities leading to injuries or performed in specific contexts where other individuals may perpetrate the offence against occupational safety and health provisions. On this purpose, the following two important tools of management and control inspired the Company:

- ✓ Risk assessment required by current regulation on occupational safety and health;
- ✓ BS OHSAS 18001:2007.

Risk assessment allowed to identify the relevant conditions where offences may be perpetrated.

The effective implementation of an Occupational Safety and Health Management System, in compliance with BS OHSAS 18001:2007, is seen by the regulator as the right formality to achieve occupational safety goals; therefore, as per art. 30 of D.Lgs. no. 18/2008, an organisational model designed accordingly may be an eligible waiver, pursuant to D.Lgs. no. 231/2001.

The Company adopted an Occupational Safety and Health Management System inspired to the BS OHSAS 18001:2007 with the aim to control its activities and their compliance with safety and health laws and regulations, international and local, as well as to organize the overall structure. Control measures envisaged by the system are in addition to the provisions of the current Special Section.

4.2. Sensitive activities

4.2.1. Categories of Sensitive activities

Sensitive activities, relevant to art. 25-septies of D.Lgs. 231/2001, are divided in the following two categories:

- ✓ *Activities exposed to risk of injury or occupational disease*, supported by the Risk Assessment Documents elaborated by the employer as per art. 28 of D.Lgs no. 81/2008. They include activities where injuries and occupational disease may occur;
- ✓ *Activities subject to the risk of offence* include those activities potentially leading to the perpetration of offences set forth by art. 25-septies of Decree, when their omission or ineffective performance may determine a negligent conduct. These activities represent a key element to adopt and effectively implement a system suitable to match all the requirements of the occupational safety and health regulations. The Company has implemented a control and risk self-assessment plan to identify all these activities and determine any eventual divergence from the system.

4.2.2. Activities exposed to risk of injury or occupational disease

A careful analysis of the structural and organisational aspects of the Company led to identify risks related to the occupational safety and health.

The results of this analysis are included in specific risk assessment reports along with indications on prevention measures required to remove or minimise their risk profiles. Therefore, more detailed information on all the activities may be found in the aforementioned reports.

These reports are constantly updated, according to the procedures of the Model, to reflect eventual new need of prevention. Furthermore, on the basis of the results of this analysis and current controls, a set of conduct rules and prevention protocols have been identified in order to prevent the omission or inefficiency of controls on occupational safety and health, which may lead to the previously mentioned offences.

4.2.3. Activities subject to the risk of offence

The current paragraph lists all relevant activities potentially leading to the perpetration of offences, set forth by art. 25-septies of Decree, when their omission or ineffective performance may determine a negligent conduct. They have been identified in accordance with provisions of art. 30 of D.Lgs. no. 81/2008 and in compliance with requirements of BS OHSAS 18001:2007:

- ✓ Identify applicable laws for technical standards;
- ✓ Define resources, duties and responsibilities of the activities related to the implementation of procedures and instructions on occupational safety and health;
- ✓ Risk assessment and relevant prevention and protection measures;
- ✓ Identify and manage group/individual protection measures to mitigate/remove risks;
- ✓ Emergency, fire prevention and first aid management;
- ✓ Procedures and instructions to control specific risks;
- ✓ Health surveillance;
- ✓ Competence, information, training and awareness of employees;
- ✓ Maintenance aimed to comply with technical standards as well as occupational safety and health standards;
- ✓ Management of contractors and control on purchases and certifications;
- ✓ Communication, participation, consultation and management of periodic meetings on occupational safety; discussion with employee representatives on occupational safety;
- ✓ Management of documentation and recording systems to ensure traceability of activities.

The list is periodically updated to include any eventual new requirement of prevention.

5. Prevention protocols

5.1. General prevention protocols

The Model shall not replace the provisions and responsibilities set forth by D.Lgs. 81/2008 and other relevant laws. Instead, it represents an additional tool to control and verify effectiveness and adequacy of the structure and organisation with current regulations on occupational safety and health.

All recipients of the Model, already identified under the General Section, shall conducts in compliances with the Ethical Code of the Company and relevant regulations on occupational safety and health, in order to prevent the aforementioned offences of manslaughter and bodily harms.

Employees and external subjects legitimately within the Company's premises shall comply with specific principles and conduct rules. In particular, any recipient of the Model, legitimately within the Company's premises, shall have the following conduct in relation to his/her experience, skills, instructions and tools provided by the Company:

- ✓ Refrain from reckless behaviours to preserve health and safety;
- ✓ Comply with regulation and corporate procedures by putting in place any relevant control to protect health and safety of collaborators and third parties, when entering the Company's premises;
- ✓ Use properly machinery, equipment, tools and any hazard material, transportation and other safety tools;
- ✓ Use properly safety and protection tools;
- ✓ Report promptly to the person in charge (depending on duties) any malfunction of the machinery and tools previously mentioned as well as other eventual hazards detected;
- ✓ Intervene, according to his/her own competencies and capabilities, when an hazard is detected;
- ✓ Attend any scheduled medical check;
- ✓ Attend any scheduled training program;
- ✓ Comply with relevant duties required by competent authority or needed to prevent occupational safety and health.

Furthermore, it is strictly forbidden:

- ✓ Behaviours potentially leading to offences ruled by the Decree;
- ✓ Breach of any protocol of the current Special Section as well as general internal regulation on occupational safety and health;
- ✓ Behaviours that may unduly influence the opinion/judgement of supervisory entities during inspections;

- ✓ Remove or change, without authorisation, any safety or control tool;
- ✓ Perform any action, out of the duties assigned, which may put at risk anyone's safety;
- ✓ Do not comply with laws and regulations on occupational hygiene, safety and health or behaviours, which may potentially create hazards.

5.2. Specific prevention protocols

The Risk Assessment Report provides specific prevention measures of injuries and occupational diseases; please refer to the Report for any detailed information.

The current organisational, management and control model is adopted and implemented in order to ensure full compliance with all relevant legal requirements on occupational safety and health.

The following principles and protocols shall apply when adopting and implementing the organisational, management and control model.

- **Identify applicable laws for technical standards**

Compliance with current law (laws, technical provisions and regulations, etc.) is ensured by formalising specific activities aimed to:

- ✓ Identify relevant laws for the Company;
- ✓ Control regulatory update;
- ✓ Assess periodically compliance with applicable law.

- **Define resources, duties and responsibilities of the activities related to the implementation of procedures and instructions on occupational safety and health**

All relevant persons in charge of managing issues on occupational safety and health shall comply with specific technical requirements (which may be imposed also by the law); such requirements shall be fulfilled in advance and may be achieved also through specific training; they shall also be fulfilled at any time.

For example:

- ✓ Responsibilities on management, coordination and control shall be formalised;
- ✓ Identification of relevant persons, as required by law, in charge of occupational hygiene and safety (including those subjects listed by Section IV of D.Lgs. 81/2008 for construction sites) and attribution of powers to perform their roles;
- ✓ The attribution and nature of powers is in line with responsibilities and severity of potential risks;
- ✓ There is segregation of duties between subjects who make decisions and perform controls;

- ✓ Any person appointed in accordance and under the occupational hygiene and safety regulation shall possess adequate and suitable competences.

When needed, the responsibilities may be delegated, according to art. 16 of D.Lgs 81/2008, with a written act clearly identifying date, characteristics, limits and budget expense.

- **Risk assessment and relevant prevention and protection measures**

Risks are identified and assessed with fairness and in compliance with principles of accuracy and completeness. According to relevant laws, the employer is responsible although other subjects may be delegated, such as the Person in Charge of Protection and Prevention Service and the relevant practitioners.

All data and information required to assess risks and identify relevant safety measures (e.g. technical documentation, opinion pools results, etc.) shall be clear, complete and truly represent the Company,

All data and information shall be collected and promptly elaborated under the supervision of the employer or other subjects with relevant technical and professional competence. Upon request, any document and relevant sources shall be provided as well.

The elaboration of the Risk Assessment Report and the plan of prevention measures may not be delegated and shall be produced by the employer, in accordance with criteria envisaged by art. 28 of D.Lgs. 81/2008. These criteria are part the documentation and cover the following features:

- ✓ Routine and non-routine activities;
- ✓ Activities of all the employees (and third parties) with access to the Company's premises;
- ✓ Human behaviour;
- ✓ External dangers;
- ✓ Hazard from transactions or surrounding environment;
- ✓ Infrastructure, tools and equipment available at Company's premises;
- ✓ Amendments to processes and/or management system, including temporary changes and their impact on transactions, processes and activities;
- ✓ Legal duties applicable on risk assessment and implementation of control measures;
- ✓ Design of workplace, machinery and equipment;
- ✓ Operational procedures.

- **Identification and management of group/individual protection measures to mitigate or remove risks**

Following the risk assessment required by the Risk Assessment Report and Operational Plan on Safety, when performing activities within the scope of Section IV of D.Lgs. no. 81/2008, it must be identified any group or individual protection measure to mitigate risks. The risk assessment process shall:

- ✓ Identify the activities where it is mandatory the use of PPE (Personal Protective Equipment);
- ✓ Define criteria to select suitable PPE in accordance with the type of risk mapped during the assessment stage and their compliance with technical rules (EC labelled);
- ✓ Delivery and storage of PPE;
- ✓ Schedule maintenance of PPE.

- **Emergency, fire prevention and first aid management**

Emergency management is implemented in accordance with specific plans which:

- ✓ Identify situations leading to a potential emergency;
- ✓ Determine procedures to manage emergency and prevent or mitigate any negative impact on occupational safety and health;
- ✓ Test the effectiveness of emergency management plans;
- ✓ Update emergency procedures, in case of accidents or negative outcome of the tests.

There are specific emergency management plans, which determine emergency exits and implementation of signals and emergency management.

There are persons in charge of emergency; they are selected between the employees and preliminary trained according to law requirements.

Fire protection mechanisms shall be up and running according to the specific assessment of fire risk or requirements of competent authority; additionally there must be also effective health services.

The effectiveness of the plan is ensured through periodic fire simulations. Employees therefore become aware of conducts and proper fire prevention devices. Simulations shall be recorded along with any maintenance of protection system.

- **Procedures and instructions to control specific risks**

Workplaces are designed in full adherence to ergonomic, comfort and wellness principles; they are subject to regular controls in order to remove, as soon as possible, any issue potentially affecting occupational safety and health; adequate hygienic conditions shall be ensured.

Dangerous areas shall be duly signalled; access may be restricted only to those subjects properly equipped and trained.

According to the level of complexity of the activities there may be specific instructions or operational procedures in addition to instructions and manuals of machinery, equipment and material. Such specific instructions shall be provided to the employee, in particular for the activities performed at building sites, and shall be recalled within relevant Safety Plans.

- **Health surveillance**

Each employee shall preliminary comply with technical requirements (see following sensitive activity: competences, information, training and awareness) and health requirement.

The general practitioner of the Company, based on information provided by the Company and its knowledge of the workplace and duties, shall assess the medical suitability of the employee and release a full or partial suitability statement to perform functions. According to the type of work and medical assessment result, the practitioner identifies the relevant protocol of health surveillance for the employee.

All personnel is duly informed and trained on how to perform its duties. Training may be dispensed with different format (face-to-face, written, etc.) based on the Company choices and relevant laws.

Selection of trainers may be subject to specific regulatory provisions.

In any case, all the information and training activities shall be recorded; any training documentation shall be stored and may be used to propose new duties.

Training aims to:

- ✓ Ensure that any individual working for the company is competent on the basis of a suitable instruction, training or experience;
- ✓ Identify any training needs and provide training or take other actions to satisfy them;
- ✓ Assess effectiveness of training and other eventual actions and maintain records;
- ✓ Assess comprehension also with specific tests;
- ✓ Ensure personnel are fully aware of any effective or potential impact of their duties, conducts and responsibilities.

- **Maintenance aimed to comply with technical standards as well as occupational safety and health standards**

Plant, machinery and equipment having a relevant impact on health and safety may be subject to maintenance protocols, eventually defined along with manufactures. Any specific intervention shall be carried out by authorised persons only, who shall provide evidence of their competences and authorisation.

Maintenance shall be recorded.

Where plant and equipment require periodic maintenance, according to current laws, then specific external entities (such as ARPA, ASL, Inspection bodies, etc.) shall be appointed.

Maintenance shall be planned according the following activities:

- ✓ Define procedures, timelines and responsibilities required to plan and execute maintenance and periodic assessments (reported on specific records) of plan, machinery and equipment;
- ✓ Define procedures to record maintenance activities and person in charge of such recording;
- ✓ Define procedures to report any fault, relevant tools and functions in charge of the maintenance process (non scheduled maintenance).

- **Management of contractors and control on purchases and certifications**

Contracted activities and services, in relation to occupational safety and health, are ruled by art. 26 and Section IV of D.Lgs no. 81/2008.

Contractors shall satisfy technical and professional requirements, which may be also verified through CCIAA enrolment. They shall also comply with insurance and social security duties for their employees by providing also the Single Document of Regular Contribution. If needed, the contractor shall inform INAL of any partial or full change of the assured activity (given the type of service required or the information provided by the Company).

Where required by law, the contractor shall release a statement of compliance with best-practice.

With reference to suppliers, installers and external maintainers of machinery, plan and other type of safety tools and equipment to be installed within the Company's premises, there may be specific controls envisaging:

- ✓ Procedures to assess that suppliers (and their employees) are compliant with safety procedures;
- ✓ Scope of work and any impact in a written contract;
- ✓ Access and activities performed by third parties within the Company's premises, with specific assessment of any related risk and production of any relevant document (e.g. DUVRI, PSC) approved by all external subjects;
- ✓ Contractual clauses ruling any eventual failure to comply with safety provisions by third parties, relevant reporting and sanctions;
- ✓ Time and attendance recording of third parties within the Company's premises in compliance with safety principles, as eventually specified in relevant agreements;
- ✓ Traceability of any control performed by senior managers and employer in compliance with the aforementioned control procedures.

Purchases of tools, machinery and plan require preliminary check of their safety and status and shall take into account any opinion received by the employee representative.

Tools, machinery and plan shall comply with current regulation (e.g. EC labelling, warranty issued by the installer, etc.). Where required, they may be subject to initial checks and ratification.

Before using any new tool, machinery and plant, the employee shall receive adequate training.

Purchase activities aims to:

- ✓ Determine criteria and procedures to select and verify qualification of suppliers;
- ✓ Determine procedures to assess compliance of tools, plant and machinery with current laws (e.g. EC labelling), as well as criteria and procedures to set suitability requirements;
- ✓ Determine, where applicable, any preliminary check and ratification.

When purchasing services, including intellectual services (e.g. planning services), the Company shall run a preliminary check on the competences of suppliers, by assessing past experience and objective requirements (e.g. enrolment in specific registers). Their performance is assessed in accordance with internal procedures. If their activities may impact the occupational safety and health, then the Company shall implement any preliminary check required by the risk assessment procedure.

- **Communication, participation, consultation and management of periodic meetings on occupational safety; discussion with employee representatives on occupational safety**

Procedures on the involvement and consultation of personnel shall envisage the following formalities:

- ✓ Internal communication across different levels and functions;
- ✓ Communication with suppliers and visitors entering the workplace;
- ✓ Receipt and response to any communication received by third parties;
- ✓ Participation of employees, also with their representatives, by:
  - Involvement in the identification of hazards, risk assessment and design of precautionary measures;
  - Involvement in accidents investigations;
  - Consulting in the event of important changes that may materially impact health and safety.

- **Management of documentation and recording systems to ensure traceability of activities**

Management of documentation is a key requirement to effectively maintain the organisational, management and control model; proper management of documentation and recording system allow traceability and represent a proof of the effective implementation. It is furthermore important to ensure that any internal and external document (e.g. notes or products and materials) is updated and available. Management of documents and recording shall ensure availability, traceability and storage.

5.3. Supervisory duties and audit activities

5.3.1. Supervisory duties

Pursuant to art. 18, par. 3-bis of D.Lgs. no. 81/08 (supervisory duties of the employer and managers on compliance with provisions on workplace safety by persons in charge, employees, suppliers, manufactures, installers and general practitioner), the following protocols apply.

- **Supervision of persons in charge (art. 19 of D.Lgs. no. 81/2008)**

The Company adopts specific protocols that require the employer or any delegated person to:

- ✓ Schedule and perform sample checks on the effective information provided to subjects with access to areas where there is potential exposure to a serious specific hazard;
- ✓ Schedule and perform sample checks on faults reported by persons in charge as well as reports of unusual behaviours held by persons in charge;
- ✓ Control any fault of tools, machinery, PEP and other hazard situations reported by the person in charge; assess actions taken by the Person in Charge of Protection and Prevention Service and any follow up;
- ✓ Control the effective internal training of persons in charge.

- **Supervision of employees (art. 20 of D.Lgs. no. 81/2008)**

The Company adopts specific protocols that require the employer or any delegated person to:

- ✓ Schedule and perform sample checks on the effective information provided to employees with access to areas where there is potential exposure to a serious specific hazard
- ✓ Schedule and perform sample checks on faults reported by persons in charge;
- ✓ Control the effective internal training of employees;
- ✓ Control that employees are effectively going through medical assessments required by law or prescribed by the general practitioner.

Protocols for employees working outside the Company's premises include the same supervisory duties required for designers and followed during control on manufacturing and installation.

- **Supervision of designers, manufactures, suppliers, installers and maintainers (articles 22, 23 e 24 of D.Lgs. no. 81/2008)**

The Company adopts specific protocols on the following:

- ✓ Scope of work and any impact in a written contract;

- ✓ Access and activities performed by third parties within the Company's premises with specific assessment of any related risk and production of any relevant document (e.g. DUVRI, PSC) approved by all external subjects;

- ✓ Tools, machinery and plan shall comply with current regulation (e.g. EC labelling, warranty issued by the installer, etc.). Where required, they may be subject to initial checks and ratification;

- ✓ Contractual clauses ruling any eventual failure to comply on safety provisions by third parties, relevant reporting and sanctions;

- ✓ Assessment procedures for suppliers shall include compliance of their employees with safety procedures;

- ✓ Time and attendance recording of third parties working within the Company's premises in compliance with safety principles, as eventually specified in relevant agreements;

- ✓ Traceability of any control performed by senior managers and employer on compliance with the aforementioned control procedures.

- **Supervision of general practitioner (art. 25 of D.Lgs. no. 81/2008)**

The Company adopts specific protocols that require the employer or any delegated person to verify:

- ✓ Compliance of general practitioner's qualifications with the law requirements;

- ✓ Regular attendance of the general practitioner to coordination meetings with the Person in Charge of Protection and Prevention Service, employee representative and the employer on occupational safety issues, including risk assessment and social responsibility of the Company;

- ✓ Regular and constant implementation by the general practitioner of medical protocols and corporate procedures on medical supervision.

5.3.2. Audit activities to assess periodically implementation and effectiveness of procedures

There are additional controls aimed to ensure constant monitoring and effective performance of the organisational system of the Company, set in accordance with the occupational safety and health regulation. With reference to the above listed controls, additional audit activities are performed by the relevant competent function, with the eventual support of external consultants.

Activities shall ensure that:

- ✓ Internal audit are regularly scheduled and performed to assess proper implementation and effectiveness of the management system;

- ✓ Prompt management of any divergence from the system;

- ✓ Audit results to be reported to the employer.

6. Information flows to SB

Persons in charge of relevant functions shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

In particular:

- ✓ Employer, Person in Charge of Protection and Prevention Service and the general practitioner shall update periodically the SB on occupational safety and health issues;
- ✓ Person in Charge of Protection and Prevention Service meets periodically with the SB to report any relevant changes of the Risk Assessment Document and procedures of the safety management system;
- ✓ Employees, employee representatives may report to the SB of any lack or fault affecting the occupational safety and health of the Company.

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

D.LGS. N. 231/01

Special Section E

Handling stolen goods, laundering and use of money, assets or benefits of illegal origin

(Art. 25-octies of D.Lgs. no. 231/01)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

Art. 25-octies of D. Lgs. no. 231/01 was introduced by D.Lgs. no. 231/07, which has formally and substantially reviewed the money laundering regulation and extended the administrative liability of handling stolen goods, money laundering and use of money, assets or benefits whose origin is illegal (art. 648, 648-bis and 648-ter of C.P.). Law no. 186/2014 on "*Provisions on self laundering, regularization and return of funds held abroad*" integrated the D.Lgs. no. 231/01 with the offence of self laundering (art. 648-ter 1 of C.P.).

Furthermore, art. 64, par.1, letter f) of the aforementioned D. Lgs. no. 231/07 and subsequent amendments and additions, withdrawn par. 5 and 6 of art. 10 of Law no.146/06 on liability of the entity for transnational offences related to laundering and use of money, assets or benefits whose origin is illegal (art. 648-bis and 648-ter of C.P.).

Therefore, pursuant to art. 25-octies of D. Lgs. no. 231/01, the Entity is now liable for the offence of handling stolen goods, money laundering and use of illegal money and self laundering, even if the offence is perpetrated on the national territory, as long as there is an unlawful profit or benefit for the entity.

The following pages disclose the provisions of the criminal laws recalled by art. 25-octies of D. Lgs. no. 231/01 along with a short comment for each offence.

The current Special Section provides, in particular, conduct rules for any subject – Directors, senior manager, manager and employees of SNAITECH S.p.A., suppliers, consultants acting on behalf of the Company – involved in the processes and sensitive activities ("Recipients").

All Recipients of the current Special Section of the Model shall behave in accordance with the following provisions in order to prevent perpetration of any relevant offence.

2. Offences under art. 25-*octies* of D.Lgs. no. 231/01

Art. 25-octies of D. Lgs. no. 231/01 " Handling stolen goods, laundering and use of money, assets or benefits whose origin is illegal and self-laundering" has broadened the list of offences under D. Lgs. no 231/01 including: handling stolen goods, laundering, use of money, assets or benefits whose origin is illegal and self-laundering.

In more details:

- **Handling stolen goods (article 648 of C.P.)**

"*Apart from participation in the predicate offence, any person who acquires, receives or conceals money or goods which are the proceeds of a criminal offence, or who assists in acquiring, receiving or concealing such money or goods, with a view to gain for himself or another, shall be punished by imprisonment for between 2 and 8 years and by a fine of between 516 Euro and 10,329 Euro. The sanction is more severe when relates to money or other assets from aggravated robbery pursuant to art. 628, par. 3, aggravated extortion pursuant to art. 629, par. 2 or aggravated theft pursuant to art, 625, par. 1, no. 7-bis.*

The punishment shall be imprisonment for up to 6 years and a fine of up to 516 Euro if the offence is not serious.

The provisions of this article shall also apply if the person committing the offence of which the said money or goods are the proceeds is not chargeable or punishable, as well as in the absence of the legal conditions for criminal prosecution in respect of the said offence".

The article is intended to punish any subject who purchases, receives or conceals money or other assets resulting from any crime. Therefore, the offence of handling stolen goods may be committed with three different conducts:

- ✓ Purchasing, through negotiation, for free or against payment;
- ✓ Receiving, with any mean and also temporary, or being complaisant;
- ✓ Concealing or hiding the assets resulting from the offence.

The offence of handling stolen goods is introduced to limit other types of offences. The legislator punishes the conduct of receiving, purchasing, concealing money or assets whose origin is illegal or being involved in similar transactions. On this purpose, the legislator intention is to avoid consolidation of the economic damage, obstruction of investigations and contextually discouraging third party interest on the transactions. The active offender is any subject who purchases, receives or conceals money or other assets of illegal origins or assist in acquiring, receiving or concealing such money or goods, with a view to gain for himself or another. The provision does not apply to the perpetrator of the original crime where money or assets came from. The object of the offence is the money or assets of illegal origin. Jurisprudence includes services and know-how although is divided on fixed real estate assets.

The wording "*purchases*" and "*receives*" include any action taken by the offender to hold the illegal goods. Concealing relates to hide such money or assets. It is furthermore important the action of assisting in acquiring, receiving or concealing assets, which may simply requires the subject to introduce, also indirectly, both parties. The subjective element of the offence, or the psychological profile of the offender, focuses on the awareness of the illegal origin. This does not imply full knowledge of the original offenders or offences and it relates to the simple awareness of the illegal origin. It is under discussion if doubt shall be considered in relation to such offence. Furthermore, art. 648 of C.P. requires that the perpetrator must act with malice, i.e. knowingly and with the intent of obtaining a profit for himself or others. Any benefit (including of political or moral nature) may be pursued with such crime. In case of absence of malice there may be the offence of unwary purchase (art. 712 of C.P.).

In relation to the conducts relevant for the D. Lgs. no. 231/01, for example, the offence may include situations where employees, who are authorised to purchase goods, omit internal procedures (or ignore their results) and knowingly purchase (in the interest of the Company) goods of illegal origin at a price sensibly lower than market price. For example, an employee decides to purchase goods, more convenient from an economic perspective, despite he/she is aware of the incomplete or wrong documentation and accepts the risk of illegal origin of the goods.

- **Money laundering (article 648-*bis* of C.P.)**

"*Apart from participation in the predicate offence, any person who substitutes or transfers money, goods or assets obtained by means of intentional criminal offences, or who seeks by any other means to conceal the fact that the said money, goods or assets are the proceeds of such offences, shall be punished by imprisonment for between 4 and 12 years and by a fine of between 5,000 Euro and 25,000 Euro.*

The punishment shall be increased if the offence is committed in the course of a professional activity.

The punishment shall be decreased if the money, goods or assets are the proceeds of a criminal offence for which the punishment is imprisonment for up to 5 years.

The final paragraph of article 648 shall apply".

The offence punishes any conduct or process allowing to conceal the illegal origin of a profit, such that it would be considered as legal. In other words, the ratio of art. 648-bis of C.P. aims to sanction transactions implemented to simulate legal origin of assets whom origin is illegal.

On this purpose, the provision also prevents any reinvestment of illegal amounts in legal activities and investments.

The provision punishes any person who substitutes or transfers money, goods or assets obtained by means of intentional criminal offences. Therefore, laundering may be perpetrated by the following conducts:

- Substitution of money, goods or assets of illegal origin with other assets;

- Transferring, including any action to move money or other assets of illegal origin and prevent leaving a trail of incriminating evidence.

Contrasting money laundering is crucial when counteracting organised crime, which usually sees two important steps: the acquisition of illegal assets and the subsequent "laundering", implemented to simulate legal origin of assets whom origin is illegal.

The offence relates to different assets including justice, public heritage and economic and public order.

The offence punishes any person who, apart from participation in the predicate offence, substitutes or transfers money, goods or assets obtained by means of intentional criminal offences, or who seeks by any other means to conceal the fact that the illegal money, goods or assets are the proceeds of such offences.

Similarly to the offence of handling stolen goods, money laundering requires that money or assets (including companies, financial instruments and receivables) originate from a previous not culpable offence (e.g. tax crimes, crimes against public heritage, etc.). The substitution of money, goods or assets of illegal origin relates to "conceal" illegal origin of the assets to subsequently replace them.

Transferring relates to the action of moving money or assets of illegal origin to prevent leaving a trail of incriminating evidence. Furthermore, it is punished any tentative to prevent leaving a trail of real origin of money and other goods.

The subjective element of the offence focuses on the awareness of the illegal origin and the intention to perpetrate the afore mentioned conducts (substitution, transfer and other conducts which prevent leaving a trial of money and other goods).

For example, the offence may be perpetrated by an employee who, after having received goods or money of illegal origin, implements the following actions:

a) ***in case of goods received,*** these are used by the Company (e.g. use of stolen computers);

b) ***in case of money,*** it is used to purchase goods and services for the Company (e.g. use of money resulting from a previous tax crime to purchase goods and services for the Company).

- **Use of money, goods or assets of illegal origin (article 648-*ter* of C.P.)**

"*Apart from participation in the predicate offence and from the cases as per articles 648 and 648bis, any person using for economic or financial activities money, goods or assets obtained by means of a criminal offence, shall be punished by imprisonment for between 4 and 12 years and by a fine of between 5,000 Euro and 25,000 Euro.*

The punishment shall be increased if the offence is committed in the course of a professional activity.

The punishment shall be decreased pursuant to paragraph 2 of article 648.

The final paragraph of article 648 shall apply".

The current offence aims to:

- Prevent transformation of illegal money into legal money;
- Use of laundered money in legal activities.

The first paragraph of art. 648-ter of C.P. excludes those subjects who participated in the predicate offence or perpetrated the offences of handling stolen goods or money laundering (art. 648 and 648-bis of C.P.). Therefore, the offence is perpetrated, differently from the other aforementioned offences, when the offender uses illegal assets for economic and financial activities[1].

Finally, art. 648-ter of C.P. envisages an aggravating circumstance, when the offence is committed in the course of a professional activity, and a mitigating circumstance, when the money or assets result from an offence punishable with prison sentence lower than five years.

The offence relates to public heritage and economic and public order.

Apart from the cases as per articles 648 (handling stolen goods) and 648-bis (money laundering), it is punished any person who uses, for economic or financial activities, money, goods or assets of illegal origin, unless the offender participated in the offence (e.g. theft, tax crime, etc.).

The concept of "use" includes any utilisation of illegal amount (in addition to the simple investment). Reference to "economic and financial activities" refers to any sector where it is possible to obtain profits.

The subjective element of the offence focuses on the awareness of the illegal origin and the intention to perpetrate the aforementioned conducts. Theoretically, the offence may be perpetrated by employees who knowingly receive goods or money of illegal origin (for example, following negative results of internal procedures, they are aware that money was transferred from/to bank accounts held by individuals or companies included in the antiterrorism list) and use them to invest, also with the support of brokers.

- **Self-laundering (article 648-*ter*.1 of C.P.)**

"*It is punished with a prison sentence from two to eight years and a fine from 5,000 Euro to 25,000 Euro any person who, perpetrated or participate to perpetrate a non culpable crime, use, substitute, transfer in economic, financial activities or speculate those money or goods, resulting from the offence perpetrated, in such a manner to prevent leaving a trail of incriminating evidence.*

Prison sentence from one to four years and a fine from 2,500 Euro to 12,500 Euro apply if the money, goods or assets are the proceeds of a criminal offence for which the punishment is imprisonment for up to 5 years.

Sanctions of the first paragraph apply when the money, goods or assets are the proceeds of a criminal offence perpetrated according to article 7 of D.L. no. 152 of 13 May 1991 converted into law no. 203 of 12 July 1991 and subsequent amendments.

[1] The word "use" include utilisation of any type and for any purpose. However, the provision is mainly intended to prevent possible alternation of the economic system and therefore the use of assets is mainly relevant with the purpose of obtaining a profit. Therefore, wording "economic and financial activities" shall refers to any sector where it is possible to obtain profits.

Except in the cases set out above, no sanctions apply if the money, goods or other benefits are used or enjoyed for personal purposes.

The punishment shall be increased if the offence is committed in the course of a professional activity.

The penalty is reduced by up to half if the perpetrator effectively strives to limit the effects of the consequences or ensure evidence as to the offence and the determination of the money, goods and other benefits originating from the offence.

The last paragraph of article 648 shall apply".

The provision punishes "*any person who, perpetrated or participate to perpetrate a non culpable crime, use, substitute, transfer in economic, financial activities or speculate those money or goods, resulting from the offence perpetrated, in such a manner as to prevent leaving a trail of incriminating evidence.".*

The provision aims to freeze the unlawful amount held by the offender and to prevent any further circulation, which may damage economic and public order. Availability of illegal money allows the offender to use them in other illegal activities or acquire privileged positions against competition (therefore altering market rules).

The list includes money and other goods or real estate assets with a relevant value.

The legislator punished any type of conduct devoted to conceal illegal money in the economic system and to "*prevent leaving a trail of incriminating evidence*": any use, substitution and/or transformation makes extremely difficult to track the illegal origin of the money or assets.

Sanction increases when money or goods result from non culpable offences punishable with a prison sentence up to five years, or if the offence is perpetrated in the course of a banking, financial or professional activity.

The penalty is reduced up to half, if the perpetrator effectively strives to limit the effects of the consequences or ensure evidence as to the offence and the determination of the money, goods and other benefits originating from the offence.

No sanctions shall apply if the money, goods or other benefits are used or enjoyed for personal purposes.

The provision of last paragraph of art. 648 of C.P. ("Handling stolen goods") applies. Therefore it is punished also the "*person committing the offence, of which the said money or goods are the proceeds, is not chargeable or punishable, as well as in the absence of the legal conditions for criminal prosecution in respect of the said offence*".

3. Focus on Self-laundering offence

Law no. 186 of 15 December 2014 introduced several provisions on regularization and return of funds held abroad as well as self laundering (by introducing the latter in the art. 648-ter.1. of C.P.).

Therefore, this offence is part of a broader system designed to counteract the consolidation of an unlawful situation, limit the circulation of illegal money or goods in legal activities and prevent leaving trials of incriminating evidences.

The perpetration of a self-laundering offence, as ruled by art. 648-ter.1 of C.P., requires that any saving of illegal origin (assumption) – for example illegal tax saving following perpetration of offences set forth by D. Lgs. no.74/2000 or illegal saving from unlawful execution of public supply contracts – is then used in business activities with the aim to prevent leaving trials of incriminating evidence.

However, it is not realist to consider any offence eligible for self-laundering as this would require the implementation of a control model able to face any kind of risk. Indeed, this situation should require to adopt organisational models in an uncertain scenarios without objective criteria. Furthermore, it would also violate the principles of legality and mandatory nature of criminal law, as recalled also by art. 2 of the Decree, which state that the entity may not be deemed liable of an offence if its administrative liability and sanctions are not ruled by laws in force before perpetration of the offence.

Notwithstanding the above consideration and given the specific reference to constitutional guarantees – recalled by the criminal law – the Company, on a prudential basis, considered appropriate to introduce protocols to strengthen the control systems on tax issues.

4. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Business support;
- Administration, Finance and Audit;
- Compliance/AML;
- Procurement of goods and services;
- HR;
- IT;
- Occupational safety and health.

5. Sensitive activities related to handling stolen goods, laundering and self-laundering, use of money, assets or benefits of illegal origin

From the analysis conducted by SNAITECH within each Division and Unit, the activities potentially exposed to perpetration of offences may be classified as follows:

- Activities exposed to "**direct risk of perpetrating the offence**" including any activity which may lead to perpetration of one or more crimes related to handling stolen goods, laundering and self-laundering, use of money, assets or other benefits of illegal origin;
- Activities that may "***contribute to perpetrating***" the offence of self-laundering or other activities which may produce illegal profits (or saving) to be used in business activities with the aim to prevent leaving trials of incriminating evidence.

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to corporate offences, pursuant to articles 25-octies of the Decree:

- ✓ Management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;

- ✓ Management of relations with clients/partners in the retail space (gaming machine owners, retailers, independent associations, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;

- ✓ Management of relations with final customers, including set up of minimum requirements, due diligence, qualifications, screening and management of contractual agreement and finalisation of the gambling account;

- ✓ Acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events);

- ✓ Management of the procedures for the procurement of goods and services (including screening of suppliers);

- ✓ Management of direct and indirect taxation;

- ✓ Treasury activities including cash movements of bank accounts;

- ✓ Management and recording credit and debit invoices and receipts;

- ✓ Management of extraordinary corporate finance transactions (e.g. investment, bond issuance, transactions of financial instruments, investment or sale of shareholding in other undertakings, purchase or sale of undertakings or business units, mergers, splits, etc.);

- ✓ Management of intragroup relations (investments, contracts, information flows, etc.);

- ✓ Management of the AML procedure (risk profiling of customers, due diligence, storage and reporting to UIF, handling SOS and PEP, etc.).

- ✓ Management of residual betting and relations with bookmakers at the end of the horseracing event, including storage of *borderau* and update of MIPAAF account;
- ✓ Management of real estate assets rented to horserace operators (e.g. restaurant, clinic, golf, etc.);
- ✓ Management of horseracing events and other events (concerts, markets, etc.): selection of counterparty, assessment, management of contractual agreement and support of supplier.

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

6. Specific prevention protocols

For transactions related to: **management of relations with business partners (Gaming machines, financial institutions, etc.); management of relations with clients/partners in the retail space (gaming machine owners, retailers, independent associations, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement; management of intragroup relations (investments, contracts, information flows, etc.)**. The provisions of par. 5 of Special Section B - Corporate offences – apply in relation to the sensitive activities.

For transactions related to: **management of relations with final customers, including set up of minimum requirements, due diligence, qualifications, screening and management of contractual agreement and finalisation of the gambling account**. Protocols include the following steps:

- ✓ Before opening gambling accounts, all subjects involved in the on-boarding process shall run an accurate due-diligence in accordance with KYC principles. In case of potential suspects on customers, additional investigation shall be conducted as per internal procedures;
- ✓ Gambling account may be opened directly on the website www.snaitech.it, by filing specific form and providing relevant information (including social security number and ID), or at SNAITECH point of sale, by showing ID and social security card;
- ✓ SNAITECH transmits to ADM all customer's data provided during the account opening and SOGEI verifies the validity of social security number;
- ✓ Providing incomplete or false information, including not providing the ID within 30 days from the opening of the account, leads to the gambling account suspension until missing information is provided within 60 days (after 60 days the account is closed);
- ✓ Online Business Unit controls the accuracy and completeness of the documentation received as well as compliance with duties. Thereafter, it records client position and relevant data;
- ✓ The right to collect winnings is subordinated to provide valid copy of ID and social security number;

- ✓ Limits may be set up for gambling accounts according to regulations, SNAITECH indications or self-exclusion choices;
- ✓ Constant monitoring of the relations with clients, by periodically updating customer information and reviewing, if necessary, the overall position;
- ✓ The Company implements, if necessary, a profiling procedure;
- ✓ The Company implements adequate internal controls to prevent money laundering;
- ✓ The Company adopts adequate tools to collect customer information, in order to assess risk profile related to money laundering;
- ✓ Customer information are collected by filing a customer due-diligence survey;
- ✓ Information are analysed and assessed by the Company for customer classification purposes and stored in relevant archives;
- ✓ The whole process is traceable (electronic and paper-based documentation) to retrace eventually responsibilities and decisions taken;
- ✓ Documentation is stored by the person in charge of relevant function.

For transactions related to: **acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events)**. Protocols include the following steps:

- ✓ Set up procedure to determine roles, activities, liabilities and controls of cash flows;
- ✓ Segregation of duties between subjects who authorise, execute and control activities;
- ✓ Prohibition to make/accept payments from subjects holding bank accounts in countries included in "Black List" or "Grey List" unless they live or work in these countries;
- ✓ Prohibition to make/accept payments from counterparties included in international and national anti-terrorism lists (available on the website http://www.bancaditalia.it/UIF/terrorismo/liste) unless there is a written authorisation by the Chief Executive Officer;
- ✓ Set up procedures for the CEO to inform and communicate with the SB of any payment made/received by counterparties included in the relevant lists;
- ✓ Bet acceptance is subordinated to validation and attribution of an univocal code produced by the national system of recording, control and validation (external to SNAITECH), set in accordance with specific gambling rules;
- ✓ Once validated, the bet is recorded (following assessment by ADM) on the gambling account with the univocal code and other data, including relevant amount;
- ✓ Winning payments credited on gambling account are communicated to the national system of recording, control and validation and to ADM;

- ✓ Accounting, recording and payment transactions on gambling accounts are executed electronically by each platform in order to retrace the overall operational process.

For transactions related to: **management of the procedures for the procurement of goods and services (including screening of suppliers); management of direct and indirect taxation; treasury activities including cash movements of bank accounts; management and recording credit and debit invoices and receipts**. The provisions of par. 5 of Special Section A – Offences perpetrated against the Public Administration– apply in relation to the sensitive activities.

For transactions related to: **management of extraordinary corporate finance transactions (e.g. investment, bond issuance, transactions of financial instruments, investment or sale of shareholding in other undertakings, purchase or sale of undertakings or business units, mergers, splits, etc.)**. The provisions of par. 5 of Special Section B - Corporate offences – apply in relation to the sensitive activities. Furthermore, additional protocols include the following steps:

- ✓ The process is formalised through internal policy or operational procedure part of the Model;

- ✓ Perform preliminary checks on the counterparty (buyer or seller) to assess identity, legal office, enrolment to Chamber of Commerce and antimafia statement pursuant to art. 10 of Law no. 575/1965;

- ✓ Perform preliminary checks on the counterparty to verify any conviction or criminal proceeding, which may result in the application of sanctions pursuant to the Decree;

- ✓ Administration and Finance Division shall preliminary verify completeness, relevancy and fairness of any supporting document for the accounting record of the transaction;

- ✓ The corporate function sponsoring the transaction or with relevant expertise, shall produce any documentation useful to support the transaction along with a preliminary report describing contents, interests and strategic goals achievable.

For transactions related to: **management of the AML procedure (risk profiling of customers, due diligence, storage and reporting to UIF, handling SOS and PEP, etc.)**. Protocols include the following steps:

- ✓ The Company adopts, if necessary, a profiling procedure to comply with anti-money laundering regulation;

- ✓ The Company implements adequate internal controls to prevent money laundering;

- ✓ The Company adopts adequate tools to collect customer information, in order to assess risk profile related to money laundering;

- ✓ Customer information is collected by due-diligence survey and submission of relevant AML documentation;

- ✓ Information is analysed and assessed by the Company for customer classification purposes and stored in relevant archives;

- ✓ Functions involved in the KYC activities collaborate with relevant authorities in relation to any suspicious transaction of money laundering or terrorism financing;

- ✓ Persons in charge of reporting, including any person who is aware of it, shall refrain from informing the subject of the reporting. In particular, it is forbidden to disclose any reporting (made, on going or to be made) on money laundering or terrorism financing, including any information received by the relevant authorities;

- ✓ The Company shall promote periodically specific training programs for employees involved, at any level, on anti-money laundering activities;

- ✓ The whole process is traceable (electronic and paper-based documentation) to retrace eventually responsibilities and decisions taken;

- ✓ Documentation is stored by the person in charge of relevant function.

For transactions related to **management of residual betting and relations with bookmakers at the end of the horseracing event, including storage of *borderau* and update of MIPAAF account**. Protocols include the following steps:

- ✓ Set up procedure to determine roles, activities, liabilities and controls on bets collection and update of MIPAAF account;

- ✓ Segregation of duties between subjects who authorise, execute and control activities;

- ✓ Identification of any player who bets or wins any amount up to the threshold set by the anti-money laundering regulation. A specific form shall be filled with the following information: name, surname, place and date of birth, address, social security number, ID number, date, transaction amount and type of payment – where required – used by the player or to pay the winnings: any relevant documentation required by the anti-money laundering shall be enclosed;

- ✓ Set up specific disciplinary rules to prevent money laundering and use of money, assets or other benefits of illegal origin;

- ✓ Implement specific training program of employees potentially exposed to the risk of money laundering and use of money and other assets of illegal origin;

- ✓ Documentation on national horseracing, collected at the identification stage, shall be provided to the relevant person in charge;

- ✓ Assess completeness and fairness of documentation collected for subsequent storage;

- ✓ Finance Director shall periodically check and sign the summary of the MIPAAF account;

- ✓ Finance Directors shall periodically check and sign the list of payment to MIPAAF;

- ✓ Cash inflows and outflows shall always be traceable and backed by documentation.

For transactions related to: **management of horseracing events and other events (concerts, markets, etc.): selection of counterparty, assessment, management of contractual agreement and support of supplier; management of real estate assets rented to horserace operators (e.g. restaurant, clinic, golf, etc.)**. Protocols shall include the following steps:

- ✓ Beneficiary of any contractual relationship shall be identified and verified;
- ✓ Set up specific warnings of risks or suspicious transactions with suppliers, on the basis of:
  - Profile of the counterparty (e.g. previous criminal convictions; doubtful reputation; direct statement from the counterparty on any involvement in criminal activities)
  - Conduct of the counterparty (e.g. ambiguous behaviour, missing data or rejection to provide data required by the transaction);
  - Location of the counterparty (e.g. off-share based counterparty);
  - Economic and financial profile of the transaction (e.g. unusual transactions by type, frequency, timing, amount and location);
  - Details and scope of the transaction (e.g. use of dummy counterparty, change of standard agreements, scope of the transaction).
- ✓ Payments to suppliers/consultants shall occur after preliminary authorisation of the person in charge of relevant function competent of the purchase and following an internal authorisation process;
- ✓ Selection and assessment of the counterparty shall be made in accordance with requirements fixed by the Company and eventually updated regularly; the Company shall fix criteria to remove parties from the counterparty list; inclusion or removal from the list may not be decided by a single subject and shall always be justified;
- ✓ If the counterparty rejects any principle of Model or Ethical Code, the Company shall terminate the contract or refrain from execution;
- ✓ Contracts with third parties shall include specific clauses with clear liabilities when incompliant with principles of the Model and Ethical Code. If needed, the contract may impose also certain information duties towards the SB.

7. Information flows to SB

Persons in charge of relevant functions shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

8. Whistleblowing procedure

The D. Lgs. no. 90/2017 amended laws on money laundering and terrorism financing, by introducing (in art. 48 of D. Lgs. no. 231/2007) a whistleblowing system similar to the one introduced by Law no. 179/2017 (in art. 6 of D. Lgs. 231/01). Both provisions impose to design specific procedures, which ensure employees and other subjects to report internally, any wrongdoing (potential or real) related to money laundering and terrorism financing.

In particular, art. 48 of D. Lgs. no. 231/2007 envisages that any channel used to report wrongdoing shall preserve the identity of whistleblower (similarly to the provisions of the Model).

To ensure the effectiveness of the whistleblowing system, the Company adopted a specific procedure "Reporting wrongdoing", which includes provisions of the Model adopted by the Company and provisions of money laundering and terrorism financing law.

In particular, to comply with the requirements of confidentiality, as per art. 48 of D. Lgs. no. 231/2007, the Company implemented a specific software available on the intranet and able to ensure confidentiality of reporting. The application allows whistleblower to specify the object of the reporting (breaches of the Model or anti-money laundering provisions): in case of reporting pursuant to art. 48 of D. Lgs. no. 231/2007, the system informs on an anonymous basis the SB.

More details are available on "Reporting wrongdoing" procedure and par. 3.8 "Whistleblowing" of the General Section of the Model.

9. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

D.LGS. N. 231/01

Special Section F

Computer crimes
(Art. 24 bis of D.Lgs. no. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premises

The current Special Section relates to the offences set forth by art. 24-bis of D. Lgs. no. 231/2001, which was lately introduced by Law no. 48 of 18 March 2008 "Acknowledgement of EU convention on computer crimes (Budapest, 23 November 2001) in the national regulation".

The current Special Section provides, in particular, conduct rules for any subject – Directors, senior manager, manager and employees of SNAITECH S.p.A., suppliers, consultants acting on behalf of the Company – involved in the processes and sensitive activities ("Recipients").

All Recipients of the current Special Section of the Model shall behave in accordance with the following provisions in order to prevent perpetration of any relevant offence.

2. Offences under art. 24-bis of D.Lgs. no. 231/2001

Provisions set forth by art. 24-bis relate to the following two categories of offences:

a) computer-related offences;

b) content-related offences.

2.1. Computer-related offences

Crimes belonging to this category share several common elements, such as:

i. ***Objective element:*** despite different behaviours or conducts, these offences have in common the computer or computer system. Indeed, computer or computer system may be used to perpetrate the offence or may be the object of the offence (against computer or computer system). Computer system means "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" (Cass. Sez. VI Pen, 4 October - 14 December 1999, n.3067, and recently Cass. Sez. V Pen., 6 February 2007, n. 11689). Data are stored, through electronic signal, on specific memories and represent combination of bits: they represent facts, information or concepts in a form suitable to be processed by a computer system, including a program suitable to cause a computer system to perform a function; "telecommunication system" means any telecommunication network, public or private, national or international, based in Italy or outside.

ii. ***Subjective element:*** it may be required an intent to defraud (awareness and intention to perpetrate the offence), or similar dishonest intent, before criminal liability applies or a specific intent to defraud (an additional fraudulent or dishonest intention to perpetrate the offence: e.g. to procure an economic benefit).

Each article of the criminal law, recalled by art. 24-bis of the Decree, is now excerpted hereinafter along with a short comment.

---

1. Budapest convention of 2001, art. 1, lett. a) states that computer system is "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*".

- **Unauthorised access to telecommunication or computer systems (art. 615 *ter* of C.P.)**

"Anyone who accesses to a computer or telecommunication system protected by security measures without authorisation, or retains access thereto against the will of any person who is entitled to deny such access, shall be punished with prison sentence up to three years.

The prison sentence may range from one to five years:

1) if the crime is committed by a public official or by a person in charge of public service, who abuses of his/her power or violates his/her duties, or by a person who acts as private investigator - even without a licence - or abuses of his/her office of system administrator.

2) if the offender perpetrates the crime through violence upon things or people or if he/she carries weapons.

3) if the offence causes the destruction or the damage of the system or the partial or total interruption of its functioning, or rather the destruction or damage of the data, the information or the programs contained in it.

If the offences of par. 1 and 2 refers to computer or telecommunication systems of military interest or (concerning) public order or public security or civil defence or other public interest, the sanction is respectively a prison sentence from one to five years and from three to eight years. For the offence under par. 1, the sanction applies upon formal compliant of the offended person; in the other cases the proceeding shall be started ex officio".

The offence is perpetrated when a subject abusively gains access to a computer system or telecommunication system protected by security measures.

On this purpose the legislation's intention is to punish any unauthorised access to a computer or telecommunication system regardless of any damage caused (for example an unauthorised access to a computer system to print, copy or read documents).

The offence is furthermore perpetrated when the offender, even if authorised, retains access to the system against the will of the system administrator.

The offence may occur for example when an employee abusively gains access, with a stolen password, to a competitor computer system and accesses confidential data pertaining to a negotiation.

- **Unauthorized possession and distribution of computer or telecommunication systems' access codes (art. 615 quater of C.P.)**

"Any person who, in order to obtain personal profit or profit for others or to cause damage to others, illegally obtains, reproduces, distributes, communicates or delivers codes, keywords or other methods suitable to access a system protected by security measures, or provides information for such purposes, is punished with a prison sentence up to one year and a fine up to Euro 5,164.

If one of the circumstances under number 1) and 2) of fourth paragraph of art. 617-quater applies, then the prison sentence is from one to two years and fine may range from Euro 5,164 to Euro 10,329"

The offence is perpetrated by any person who, in order to obtain personal profit or profit for others or to cause damage to others, illegally obtains, reproduces, distributes, communicates or delivers codes, keywords or other methods suitable to access a system protected by security measures, or provides information for such purposes.

Art. 615-quater of C.P. therefore punishes behaviours held ahead of the unauthorised access, which result in distributing access codes to computer systems.

Password or codes may allow access to computer system.

It is furthermore punished the person who provides information allowing to reproduce access codes or breach security measures.

The offence may occur for example when an employee, after having obtained login credentials, distributes relevant access codes or password to computer system of competitors.

- **Distribution of computer equipment, devices or programmes aimed at damaging or interrupting a computer or telecommunication system (art. 615 quinquies of C.P.)**

"Anyone who, in order to unlawfully damage a computer or telecommunication system, the computer data or programmes contained therein or pertaining thereto, or to contribute to the total or partial interruption or alteration of its functioning, manages to obtain, produces, reproduces, imports, diffuses, communicates or in anyway puts at the disposal of others computer equipment, devices or programmes shall be sentenced to imprisonment of up to two years and to a fine of up to 10,329 euros"

The offence is perpetrated by anyone who, in order to unlawfully damage a computer or telecommunication system, the computer data or programmes contained therein or pertaining thereto, or to contribute to the total or partial interruption or alteration of its functioning, manages to obtain, produces, reproduces, imports, diffuses, communicates or in anyway puts at the disposal of others computer equipment, devices or programmes.

The offence may occur for example when an employee runs an hacker attack to alter data of competitors.

- **Wiretapping, blocking or illegally interrupting computer or information technology communications (art. 617-quater of C.P.)**

"Anyone who, fraudulently conducts wiretapping communications within a computer system or telecommunication system or between several systems, or blocking or interrupting such communications, is punished with a prison sentence from six months to four years.

Unless a major offence applies, the same sanction applies to anyone who discloses, using any mass media, in part of in full, the content of the communication as per first paragraph.

Offences under par. 1 and 2 apply upon formal complaint of the offended person.

The proceeding shall be started ex officio with a prison sentence from one to five years if the offence is perpetrated:

1) *If the offences refers to computer or telecommunication systems of the State or other public entity or companies performing public services;*
2) *if the crime is committed by a public official or by a person in charge of public service, who abuses of his/her power or violates his/her duties or abuses of his/her office of system administrator.*
3) *if the crime is committed by a person who acts as unauthorised private".*

The offence is perpetrated when a subject fraudulently conducts wiretapping communications within a computer system or telecommunication system or between several systems, or blocking or interrupting such communications or discloses, using any mass media, in part of in full, the content of the communication.

It is indeed feasible wiretapping communication, during data transmission, within a computer system or telecommunication system or between several systems to gain access or change address: the goal is typically to breach confidential information or eventually interrupt delivery.

The offence may occur for example when an employee blocks a specific data transmission to prevent a competitor from joining a tender or negotiation.

- **Installation of devices aimed at wiretapping, blocking or interrupting computer or information technologies communications (art. 617 quinquies of C.P.)**

"Anyone who, other than cases allowed by law, installs equipment designed to wiretap, block or interrupt communications, regardless of the occurrence of such events, is punished with prison sentence from one to four years.

The prison sentence is from one to five years in the circumstances envisaged by paragraph four of art. 617-quarter".

The offence is perpetrated, other than the cases allowed by law, if anyone installs equipment designed to wiretap, block or interrupt communications of a computer or telecommunication system.

The prohibition refers to the simple installation of equipment, regardless the actual usage and as long as they may potentially cause damages.

The offence may occur for example when an employee installs technological equipment (e.g. sniffer) to wiretap telephone or computer communication of a competitor.

- **Damaging of computer information, data and programmes (art. 635-bis of C.P.)**

"Provided that the conduct does not constitute a more serious offence, anyone who destroys, deteriorates, cancels, alters or suppresses any computer information, data or programmes of others shall be punished, upon complaint of the offended person, with a prison sentence from six months to three years.

If the conduct is committed by abusing the quality of system operator, the prison sentence may range from one to four years and the proceedings shall be started ex offficio".

The offence punishes any person who, destroys, deteriorates, cancels, alters or suppresses any computer information, data or programmes of others.

The offence may occur for example when an employee destroys or alters data related to a creditor of the Company with the aim to suppress any sensitive information or evidence of the payable.

- **Damaging computer information, data and programmes used by the State or any other public body or a body anyway having a public utility (art. 635-ter of C.P.)**

"Provided that the conduct does not constitute a more serious offence, anyone who destroys, deteriorates, cancels, alters or suppresses any computer information, data or programmes used by the State, public entities or other private entities of public service, is punished with a prison sentence from one to four years.

If the conduct leads to the destruction, deterioration, cancellation, alteration or suppression of the computer information, data or programmes the prison sentence may range from three to eight years.

If the conduct is committed by abusing the quality of system operator, the sentence shall be increased".

The offence is perpetrated by a subject who destroys, deteriorates, cancels, alters or suppresses any computer information, data or programmes used by the State, public entities or other entities of public utility.

Differently from previous offence, the criminal conduct includes both damages and preparation of the offence; furthermore, the damage is inflicted to the State, public entities or other entities performing public service; the crime is also perpetrated in the event of private data, information or programmes used to for public service.

The offence may occur for example when an employee destroys data held by a judicial authority in relation to a potential investigation on the Company.

- **Damaging computer or telecommunication systems (art. 635-quater of C.P.)**

"Provided that the act does not constitute a more serious offence, anyone who, through any of the conducts under Article 635-bis, or through the introduction or transmission of data, information or programmes, destroys, damages or makes in whole or in part unusable the computer or telecommunication systems of others or seriously hampers their functioning, is punished with prison sentence from one to five years.

If the conduct is committed by abusing of the quality of system operator, the sentence shall be increased".

The offence is perpetrated when a subject, through any of the conducts under Article 635-bis, or through the introduction or transmission of data, information or programmes, destroys, damages or makes in whole or in part unusable the computer or telecommunication systems of others or seriously hampers their functioning.

In the example provided earlier on art. 635-bis of C.P., the offence may lead to destruction, damage or hampering any computer or telecommunication system of third parties (e.g. competitor).

- **Damaging computer systems or telecommunication systems of public service (art. 635-quinquies of C.P.)**

"If the conduct in article 635-quater is aimed at destroying, damaging, making in whole or in part unusable any computer or telecommunication system of public service or at seriously hampering their functioning, the sanction is a prison sentence from one to four years.

If the offence leads to the destruction or damaging of the computer or telecommunication system of public service or if this is made, in whole or in part, unusable then the sanction is a prison sentence from three to eight years.

If the conduct is committed by abusing the quality of system operator, the sentence shall be increased".

The offence is perpetrated when the conduct punished by 635-quater is aimed at destroying, damaging, making, in whole or in part, unusable any computer or telecommunication system of public service or at seriously hampering their functioning.

Differently from the offence envisaged by art. 635-ter of C.P. (damaging computer information, data and programmes used by the State, public entities or a entities performing public service) here it is relevant, first of all, the damage caused to the entire system and, secondly, that the system is used for public services, regardless the private or public nature of the owner.

The offence may occur for example when an employee, by introducing or transmitting data, information or programmes, destroys computer or telecommunication system of the judicial authority (in case of a potential investigation on the Company).

2.2. Content-related offences

In relation to the category b) of crimes previously mentioned in chapter 2, they share several common elements such as:

i. ***Definition of "computer data"***: means any representation of facts, information or concepts in a form suitable for processing in a computer system, which may be used as proof of evidence (computer data is treated similarly to public deed);
ii. **Legal asset under protection**: any interest to preserve authenticity and truthfulness of items with probative value and certainty of economic and legal relations;
iii. ***Objective element****:* conduct to alter/tamper materially the document or affect the authenticity or truthfulness of its contents (forgery);
iv. ***Subjective element***: required the intent to defraud (it is therefore excluded any negligence)

- **Forgery of electronic documents (art. 491-*bis* of C.P.)**[2]

"Public or private computer documents having probative value share the same treatment applicable to forgery of traditional paper documents".

- **Computer fraud of the subject certifying electronic signatures (art. 640 quinquies of C.P.)**

"The subject certifying electronic signatures who, in order to procure for himself or for others an unlawful profit, or to damage others, infringes the obligations provided by law for the issuance of a qualified certificate, is punished with a prison sentence up to three years and a fine from 51 to 1,032 Euro".

The offence is perpetrated by any subject certifying electronic signature who, in order to procure for himself or for others an unlawful profit, or to damage others, infringes the obligations provided by law for the issuance of a qualified certificate.

---

2. This offence extended the forgery of documents (Chapter III, Title VII, Book II) to "computer documents" meaning any public or private computer documents having probative value. The relevant forgery applicable to SNAITECH are:

1. Forgery perpetrated by a private person (art. 482 of C.P.): "*If any of the offences indicated in articles 476, 477 and 478 are committed by a private individual or by a public official outside the scope of his/her duties, sanctions are reduced by one third*". The offence may occur, for example, when an employee alters bank statements on tax payments (Art. 476 of C.P.) or digital administrative certificates or authorisations (art. 477 of C.P.) or reproduce a copy of a public deed or private document, assuming the existence thereof (art. 478 of C.P.).
2. Intentional forgery committed by a private individual in public deeds (art. 483 of C.P.): "*Any person making false statements to a public official in a public document having probative value is punished with a prison sentence not lower than three months*". The offence may occur, for example, when an employee, during the process of requesting licences or authorisations (digital request), states that the Company is eligible and fulfil the relevant requirements.
3. Use of false deeds (art. 489 of C.P.): "*Any person who, while not taking part in the falsification of a deed, uses such false deed is punished with the sanctions envisaged in previous articles reduced by one third*". The offence may occur, for example, when an employee, uses false computer documents – e.g. forging electronic receipts of payment to procure profits for the Company.
4. Removal, destruction and concealment of authentic deeds (art. 490 of C.P.): "*Any person who completely or partially destroys, removes or conceals a public deed, a private agreement or a will, promissory note or similar instrument is punished respectively by art. 476, 477 and 482*". The offence may occur, for example, when an employee gains access to someone else's computer system and destroys documents having probative value.
5. Authentic copies that replace missing originals (art. 492 of C.P.): "*Pursuant to the previous provisions, "public deeds" and "private agreements" include the original deeds and authentic copies of the same when they lawfully replace the missing original copies*".

The aforementioned articles set the potential inclusion of forgery crimes. Furthermore, given the current structure of SNAITECH, its business and corporate purpose, certain provisions of Chapter III, Book III of C.P. may not apply to a public or private computer documents, defined as any representation of facts, information or concepts in a form suitable for processing in a computer system, which may be used as proof of evidence (art. 491 of C.P.). In particular: articles 476, 477, 478, 479, 480, 481, 487 and 493 of C.P.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal;
- Business support;
- IT;
- Administration, Finance and Audit;
- Compliance.

4. Sensitive activities related to Computer crimes

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to computer crimes, pursuant to articles 24-bis of the Decree:

- ✓ Management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;
- ✓ Management of terminals instalment and set up (roll-out and connectivity);
- ✓ Treasury activities including cash movements of bank accounts;
- ✓ Management and recording credit and debit invoices and receipts;
- ✓ Management of physical and logical integrity of any electronic or digital company information;
- ✓ Management of information flows to Public Administration by means of IT tools (PEC, ADM platform, AdE platform for e-invoice, etc.);
- ✓ Access to systems and authorisation to change information and data stored in the Company records (accounting, personnel, suppliers, clients, PEP, etc.);
- ✓ Purchase, development and maintenance of computer systems;
- ✓ Installation, management and use of any software, graphics, pictures without relevant authorisation or copyrights as well as playing any illegal or falsified multimedia contents within the PoS or without having paid relevant contribution to SIAE;
- ✓ Management of accidents and IT security issues related to data and information.

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Specific prevention protocols

For transactions related to the **management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement**. The provisions of par. 5 of Special Section B - Corporate offences – apply in relation to the sensitive activities.

For transactions related to: **management of terminals instalment and set up (roll-out and connectivity); treasury activities including cash movements of bank accounts; Management and recording credit and debit invoices and receipts; management of information flows to Public Administration by means of IT tools (PEC, ADM platform, AdE platform for e-invoice, etc.); access to systems and authorisation to change information and data stored in the Company records (accounting, personnel, suppliers, clients, PEP, etc.)**. The provisions of par. 5 of Special Section A – Offences against the Public Administration – apply in relation to the sensitive activities.

For transactions related to the **management of physical and logical integrity of any electronic or digital company information**, in particular for unauthorised accesses to SNAITECH S.p.A. systems perpetrated by hacker aimed at obtaining and/or tampering protected information or damaging connectivity (Cyber Attacks). Protocols include the following steps:

- ✓ ICT Divisional Head is responsible to manage Computer security;
- ✓ The Company has formalised rules on how to use computers and computer systems. These rules shall include:
  - How to safety storage and use corporate assets (PC, etc.);
  - Proper use of internet and prohibition to use networks other than corporate ones.
- ✓ Automatic lock in of programmes and computers during inactive sessions. Timing varies on the program or system used;
- ✓ Rules on how to use, select and manage antivirus for the company's network, pc and related documents;
- ✓ Each user shall access computer system through user-id and password. Credentials shall be confidential and must not be disclosed to anyone;
- ✓ The Company sets requirements for password in terms of minimum length, expiry, history, lockout and complexity. Requirements may be checked also automatically (by the program or system). Credentials shall be changed periodically;
- ✓ Password shall be encrypted;
- ✓ Non public data and information, also related to clients and third parties (trade, technical and organisational), shall be handled with confidentiality (including any remote access);
- ✓ The Company sets processes to manage new hiring, redundancy or relocation, in terms of access to computer systems;

- ✓ Track any access to computer system or data related to specific transaction (when track change is required);

- ✓ Set up, implement and communicate specific procedures to rule credentials for physical access (access codes, badges) to premises hosting computer and IT systems and any eventual track;

- ✓ Set up safety measures, surveillance and frequency of control, responsibilities, reporting process for breaches of technical premises and safety measures, any remedy action;

- ✓ In case of wireless connection to internet (WiFi), any access shall be protected using specific keys and protocols to prevent third parties access to Company routers and perpetrate wrongdoings;

- ✓ Limit remote access to the computer system by using authentication systems (e.g. VPN) in addition to the system used by employees and other authorised subjects;

- ✓ Limit access to the server room to authorised personnel only and rule third party access, if required by specific circumstances;

- ✓ The person in charge of the relevant Function shall store any documentation such that any further amendment is allowed only with specific authorisation and relevant evidence is provided (in order to ensure proper traceability of the process and facilitate any eventual subsequent control).

For transactions related to: **purchase, development and maintenance of computer systems; installation, management and use of any software, graphics, pictures without relevant authorisation or copy rights as well as playing any illegal or falsified multimedia contents within the PoS or without having paid relevant contribution to SIAE**. Protocols include the following steps:

- ✓ Formalise roles, duties and liabilities of the ICT Division;

- ✓ The Company has formalised rules on how to use computers and computer systems. These rules shall include:

  - How to safety storage and use corporate assets (PC, etc.);

  - Proper use of internet and prohibition to use networks other than corporate ones.

- ✓ Automatic lock in of programmes and computers during inactive sessions. Timing varies on the program or system used;

- ✓ Outbound communication shall be made via proxy or firewall;

- ✓ Any communication made via proxy or firewall shall be recorded in specific log;

- ✓ Access to internet via proxy server and for business purpose only;

- ✓ Formalise procedures to ensure that usage of any material under copyrights is compliant with contracts;

- ✓ Before submitting to a third party, Legal and Corporate Affair Division shall authorise any draft of the contract. In particular, the Division shall ensure the inclusion of clauses to protect copyright when purchasing from third parties;
- ✓ Employees and other authorised parties shall commit to use properly any IT asset;
- ✓ Any IT position or sub system of the Company shall be protected in order to prevent any illegal installation of equipment, which may wiretap communications within a computer system or telecommunication system or between several systems, or blocking or interrupting such communications;
- ✓ Prohibit to install and use any software ("P2P", file sharing or instant messaging), which allows exchanging files with other users over the internet (video clip, documents, songs, virus, etc.) without any control by the Company;
- ✓ Restrict access to social network, which may be used to transfer infected files;
- ✓ Rule any use of email or internet for personal reasons and fix any eventual disciplinary sanctions.

For transactions related to the **management of accidents and IT security issues on data and information**, protocols shall include the following steps:

- ✓ The Company has formalised rules on how to use computers and computer systems. These rules shall include:
  - How to safety storage and use corporate assets (PC, etc.);
  - Proper use of internet and prohibition to use networks other than corporate ones.
- ✓ Rules on how to use, select and manage antivirus for the company's network, pc and related documents;
- ✓ Formalise roles, duties and liabilities of the ICT Division;
- ✓ The Company has formalised a Disaster Recovery procedure;
- ✓ Employees and other authorised parties shall commit to use properly any IT asset.

6. Information flows to SB

Persons in charge of relevant functions shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D.LGS. 231/01

Special Section G

Offences related to organised crime
(Art. 24 ter of D.Lgs. no. 231/2001) and Transnational crimes
(art. 10 of Law no. 146/2006)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

The current Special Section rules both offences related to Organised Crime, pursuant to art. 24-ter of D. Lgs. no. 231/2001, and transnational crimes, pursuant to art. 10 of Law. No. 146/2006.

In particular, art. 24-ter of D. Lgs. no. 231/01 (introduced by art. 2 of Law no. 94 of 15 July 2009 on "Provision on public security") refers to the following offences perpetrated by Organised Crime:

- **Unlawful association to commit a crime (art. 416 of C.P.)**

"When three or more persons associate in order to commit several criminal offences, those promoting or setting up or organizing such conspiracy shall be punished, for this sole offence, with a prison sentence from three to seven years.

The simple participation to the association is punished with prison sentence from one to five years.

Those leading the association shall be liable to the same punishments as those promoting it.

If the participants in the association carry out armed raids, the sanction is a prison sentence from five to fifteen years.

The punishment shall be increased if the association includes ten or more persons.

Whenever the organization is aimed to commit any of the crimes referred to in articles 600, 601 and 602, and article 12, paragraph 3-bis of the provisions on the regulation of immigration and the status of foreigners, set forth by D. Lgs. no. 286 of 25 July 1998, imprisonment from five to fifteen years in the cases provided for in the first paragraph, and from four to nine years in the cases provided for in the second paragraph shall be applied.

Whenever the organization is aimed to commit any of the crimes referred to in articles 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 609-bis, when the crime is committed against underage, 609-quater, 609-quinquies, 609-octies, when the crime is committed against underage, and 609-undecies, the imprisonment is from four to eight years, in cases foreseen in the first paragraph, and from two to six years, in cases provided for in the second paragraph".

- **Mafia-type criminal associations (art. 416-bis of C.P.)**

"Persons belonging to a Mafia-type organisation of three or more persons shall be punished with a prison sentence from three to six years.

Persons who promote, lead or organise the association shall be punished with prison sentence from four to nine years.

A Mafia-type organisation is an organisation whose members use intimidatory power and rely on subjection and omertà to perpetrate offences, to acquire direct or indirect management or control of economic activities, licences, authorisations, public procurement contracts and services or to obtain unlawful profits or advantages for themselves or others, or to prevent or obstruct the free exercise of vote, or to procure votes for themselves or others at elections.

If the organisation is armed, members shall be liable to imprisonment for a term of between four and ten years in the circumstances described in the first paragraph and between five and fifteen years in the circumstances described in the second paragraph.

The organisation is armed if its members, to pursue their goals, access to weapons or explosives, even if hidden or stored.

If the association is directed towards committing one of the crimes under Articles 600, 601, and 602, a prison sentence of between five to fifteen years is applied in the cases foreseen in the first paragraph and from four to nine years in cases foreseen in the second paragraph.

If the economic activities, which the members intend to acquire or maintain control over, are financed in whole or in part by the proceeds of crime, the sanctions be increased from one third to half.

In the event of a conviction, instruments or means, which were used or intended to be used to commit the offence and the proceeds thereof shall be forfeited.

The provisions of this section are also applicable to the Camorra and other organisations, which make use of the intimidatory power of the association to pursue goals typical of Mafia-type organisations".

- **Bargaining of votes between politicians and members of Mafia (art. 416-ter of C.P.)**

"Whoever accepts the promise to obtain votes, through the ways referred to in the third paragraph of article 416-bis, in exchange of payment or promise of payment of money or other benefits, shall be punished with imprisonment from four to ten years.

The same punishment applies to those who promise to obtain votes in the manner specified in the first paragraph".

- **Kidnapping for ransom (art. 630 of C.P.)**

"Any person who kidnaps a person in order to obtain an unlawful profit, for himself or another, as the price of the release, shall be punished by imprisonment for between twenty-five and thirty years.

If the kidnapping results in the death of the kidnapped person and this is an unwanted consequence of the offender's part, the offender shall be punished by imprisonment for thirty years.

If the offender causes the death of the kidnapped person, imprisonment for life shall be imposed.

An accomplice, who, by withdrawing from the association, seeks to allow the victim to regain his/her freedom, without this resulting from the price of release, shall be liable to the punishments as per article 605.

Nevertheless, if the victim, once released, deceases as a consequence of the kidnapping, the punishment shall be imprisonment for between six and fifteen years.

With respect of an accomplice who, by withdrawing from the association, seeks to prevent the criminal activity from having further consequences, apart from the case referred to in the preceding paragraph, or else concretely assists police or judicial authorities in collecting evidence which is

fundamental for the identification or apprehension of the accomplices, imprisonment for between twelve and twenty years shall be substituted for life imprisonment and any other punishment shall be reduced by one-third to two-thirds.

Whenever a mitigating circumstance applies, imprisonment for between twenty and twenty-four years shall be substituted for the punishment as per the second paragraph; imprisonment for between twenty-four and thirty years shall be substituted for the punishment as per the third paragraph.

Where more than one mitigating circumstances apply, the punishment to be imposed as resulting from the application of the above reductions shall not be less than ten years in the case as per the second paragraph and not less than fifteen years in the case as per the third paragraph.

The limitations on prison sentence set out in previous paragraph may be derogated if mitigating circumstances of fifth paragraph apply".

- **Conspiracy to unlawfully engage in the traffic of narcotic and psychotropic substances (art. 74 of D.P.R. no. 309/90)**

"When three or more persons conspire to commit several criminal offences listed in art. 73, or promote, constitute, manage, organise or finance the conspiracy, they shall be punished with prison sentence not lower than twenty years.

Anyone who takes part in a conspiracy shall be imprisoned for a period of not less than 10 years.

The penalties shall be increased if the numbers of persons involved is 10 or more, or if there are abusers of the narcotic and psychotropic substances among the conspirators.

If the conspirators are armed, in the cases indicated in paragraph 1 and 2, the penalty may not be less than 24 years' imprisonment, and in the case provided by paragraph 2, not less than 12 years' imprisonment. The conspiracy shall be considered armed when the conspirators have arms or explosives at their disposal, even if these are concealed or stored elsewhere.

The penalties shall be increased in the event that the circumstances provided by art. 80, par. 1, letter e) apply.

If the conspiracy is designed to commit the offences included in art. 73, par. 5, the provisions of par. 1 and 2, art. 416 of C.P. shall apply.

The penalties provided by paragraphs 1 to 6 shall be reduced by between one half and two thirds in the case of persons who actively cooperate to provide evidence or to deprive the conspirators of resources which are essential for the commission of a criminal offence.

When the criminal offence created by s. 75 of Law No. 685 of 22 December 1975, repealed by s. 38 (1) of Law No. 162 of 26 June 1990 is referred to in Laws and Decrees, this reference shall be construed to refer to this section".

- **Offences perpetrated under conditions of art. 416-bis of C.P. to facilitate Mafia-type criminal associations (Law no. 203/91)**

- **Offences relating to the illegal manufacturing, introduction into the State, putting on sale, transfer, possession and taking into a public place or place open to the public of weapons of war or similar or parts thereof, explosives, illegal weapons as well as more common firearms (Art. 407, paragraph 2 letter a) number 5 of Italian Code of Criminal Procedure)**

In relation to Transnational Crimes, art. 3 of Law no. 146/2006 defines transnational offence any offence, punished with a prison sentence not lower than four years, where it is involved a criminal association and:

- It is perpetrated in more than one State;

- When perpetrated in a single State, it was substantially arranged, planned and managed or controlled in a different State;

- It is perpetrated in a single State and the association is involved in criminal offences in more than one State;

- It is perpetrated in a State and produces relevant impacts on another States.

Art. 10 of Law no. 146/2006 envisages an administrative liability of the entity for the following offences, when the transnational element arises:

- **Inducement not to give statement or to give an untruthful statement before the judicial authority (art. 377-bis of C.P.)**

"Unless a major offence is perpetrated, anyone who uses violence or threats, offers or promises money or other benefits to induce not to make statements, or to make false statements any person who is called before the judicial authorities to make statements in connection with criminal proceedings, if such person has the right to remain silent, then is punished with a prison sentence from two to six years".

- **Aiding and abetting fugitive (art. 378 of C.P.)**

"When an offence perpetrated is punished with life or prison sentence, any subject who, without having participated to the offence, helps the offender to avoid investigation by the authorities, including international Criminal Court, or avoid arrest, is punished with a prison sentence up to four years.

If the perpetrated crime falls under the provision of art. 416-bis, then the prison sentence may not be lower than two years.

For offences punished with a fine, the amount sanctioned may be up to Euro 5,165.

Provisions of this article apply also when the person who received aid is declared not culpable or not chargeable of the offence".

- **Unlawful association to commit a crime (art. 416 of C.P.)** [see *ut supra*]

- **Mafia-type criminal associations (art. 416-bis of C.P.)** [see *ut supra*]

- **Provisions against illegal immigration (art. 12, par. 3, 3-bis, 3-ter and 5, of D.Lgs. no. 286/1998)**

"3. Unless a major offence is perpetrated, anyone who promotes, leads, organises, finances or transports immigrants in the State's territory or contributes to the illegal entry in the State's territory, or in another State of which the person is not citizen or does not have the right to permanent residence, is punished with imprisonment from one to fifteen years and with a 15,000 Euro fine for each person in the following cases: a) entry or illegal permanence in the State's territory of five or more persons; b) the life of the person transported was placed at risk or was exposed to danger to obtain his entry or illegal permanence; c) the immigrant received inhuman or demeaning treatment to obtain his entry or illegal permanence; d) there are three or more persons involved or using international transportation services or counterfeited or modified documents or in any case obtained illegally; e) the offenders have access to weapons or explosives.

3-bis. If the offences in paragraph 3 are committed under two or more of assumptions included in letters a), b), c), d) and e) of the same paragraph, the sanction is increased.

3-ter. Imprisonment is increased from one third to half and a 25,000 Euro fine is imposed on every person if the facts as mentioned under paragraphs 1 and 3 are committed: a) with the aim to recruit persons for prostitution or other sexual or labour abuse, or entry of underage to employ in illegal activities; b) are committed for profit, even indirect.

[…]

5. Excluding circumstances ruled in previous paragraphs and unless a major offence is perpetrated, anyone who, in order to obtain an unlawful profit from illegal immigrants or other activities sanctioned by this article, favours immigrants to stay in the State's territory against provisions of this article, is punished with imprisonment up to four years and with a fine up to 30 million Euros. When the offence is perpetrated by two or more persons, or is related to five or more immigrants, the sentence is increased from one third to half".

- **Criminal associations for the smuggling of foreign tobacco products (art. 291-quater of DPR no. 43/1973)**

"When three or more persons associate in order to commit several criminal offences under art. 291-bis, those promoting, setting up, organizing or financing such association shall be liable, for this sole offence, of prison sentence from three to eight years.

Anyone taking part in a conspiracy shall be punished with prison sentence from one to six years.

The punishment shall be increased if the association includes ten or more persons.

If the conspirators are armed or provisions under letter d) or e) of par. 2, art. 291-ter apply, the prison sentence is from five to fifteen years for those circumstances identified under par. 1 while prison sentence may range from four to ten years for those circumstances identified under par. 2.

The conspiracy shall be considered armed when the conspirators have arms or explosives at their disposal, even if these are concealed or stored elsewhere.

Sanctions provided by art. 291-bis, 291-ter and by the current articles shall be reduced by one third and half in the case of persons who actively cooperate to provide evidence or to deprive the conspirators of resources which are essential for the commission of a criminal offence".

2. Offences under art. 24-*ter* of D.Lgs. no. 231/2001 and art. 10 of Law no. 146/2006

According to the analysis run by the Company, the following offences were considered relevant for the Company.

- **Inducement not to give statement or to give an untruthful statement before the judicial authority (art. 377-*bis* c.p.)**

The offence is perpetrated by anyone who uses violence or threats, or offers or promises money or other benefit to induce not to make statements, or to make false statements any person who is called before the judicial authorities to make statements in connection with criminal proceedings, if such person has the right to remain silent.

The offence is actually perpetrated when the violence or threats occur or money and other benefits are promised.

Such provision aims to ensure a rightful development of the legal proceeding by punishing any external influence, which may alter the proceeding.

- **Aiding and abetting fugitive (art. 378 of C.P.)**

Art. 378 applies when a person helps the offender, without having participated to the offence and such offence is punished with life or prison sentence, in order to avoid investigation by the authorities or arrest.

The provision requires a criminal conduct to assist anyone suspected of a criminal offence.

Provisions of this article apply also when the person who received aid is declared not culpable or chargeable of the offence. The ratio is to preserve legal proceeding from any alteration.

- **Unlawful association to commit a crime (art. 416 of C.P.)**

Structure and purpose of the association

The offence is determined by the following factors: a) stability and continuity of the association, also after the perpetration of the offence; b) goals of the association are undetermined; c) the association is properly organised and structured.

a): According to relevant jurisprudence the association may not be permanent and must not be limited to perpetrate one or more crimes. It is therefore allowed also an unlawful association established for a short time whose existence goes beyond the perpetration of the offences.

b): A broad criminal plan which involves different and potentially numberless criminal activities with the permanent involvement of all conspirators. This indeterminacy characterises such offence versus other crimes, where a temporary association is established with the specific goal to perpetrate one or more crimes.

c): part of the jurisprudence requires an organisational structure "*suitable to perform the criminal plan*", while others require basic arrangements and preparation of means to perpetrate the offences. In any case, it is unnecessary the existence of hierarchy levels and specific roles and competences.

On this basis it is worth highlighting the recent court sentence no. 41528/2010 of 28 October 2010, which states that: "*Charging the offence of unlawful association does not require a specific and complex organisation while it is required the simple arrangement of means, or using existing ones, to perpetrated the criminal plan*".

Conduct

According to art. 416 of C.P., on one side there is the intention to associate and, on the other side, there is the intention to promote, set up and organise.

On the former, the doctrine identifies a psychological element in the awareness and willingness to join conspiracy and acknowledgement of the criminal plan.

However the offence is perpetrated as long as three or more persons are involved in the conspiracy.

On the promotion, set up and organisation, the doctrine considers "promoter" any subject who promotes, alone or together with other parties, the conspiracy; "set up" refers to those activities needed to create the conspiracy; "organisation" relates to the coordination of members to perform criminal activities.

Third paragraph of the article puts on the same level the promoter and the person leading the conspiracy. However, it must be noted that the promoter and constituent may not be members of the conspiracy while the boss materially join the unlawful association.

Subjective element of the offence

The subjective element is represented by the awareness and willingness to permanently join conspiracy. However, it is required a specific fraudulent intention to contribute to the criminal activities. Instead, it is not required the will to immediately perpetrate any specific offence.

Perpetration of the offence

Particular attention is required on the timing of offence also from the administrative liability perspective. The crime is perpetrated as soon as the association is established, since, in this specific moment it becomes a threat for the public order, according to the doctrine. Therefore, for this type of crimes, it is irrelevant the timing and the effective perpetration of criminal offences.

- **Mafia-type criminal associations (art. 416-*bis* of C.P.)**

Conduct

The first two paragraphs of the article are similar to art. 416 of C.P. Therefore, the same considerations mentioned earlier apply.

The third paragraph instead introduces, for the first time ever, the concept of mafia-type association, which requires two specific criteria: **mean used** and **goal**.

On the **mean used**, the first criterion puts emphasis on the intimidatory effect resulting from the criminal reputation built up by the conspiracy with violence and oppression. It may not be necessary the perpetration of any specific intimidation by the conspirers, while it is necessary that intimidatory power results in subjection and omertà.

The second criterion (**goal**) focuses on the goal of the association, no longer committed to crimes against individual and public heritage and, now, more involved in the political environment – intimidating politicians and bargaining votes (see art. 416-ter) – and social environment, to profit from legal activities (e.g. public contracts).

In particular, the following considerations apply to the goals mentioned in par. 3 of art. 416-bis of C.P.:

- ✓ The goal "*to acquire direct or indirect management or control of economic activities, licences, authorisations, public procurement contracts and services or to obtain unjust profits or advantages for themselves or others*" includes many typical activities of the private and public sectors. The word "*management*" refers to lead activities relevant from an economic perspective while "*control*" refers to the ability of influencing the activities of an entire sector.

- ✓ Please refer to art. 416-ter on the statement "*to prevent or obstruct the free exercise of vote, or to procure votes for themselves or others at elections*".

Relations between art. 416-bis and 416 of C.P.

The two aforementioned criteria allow distinction between offences ruled under art. 416 and 416-bis of C.P.

As per the mean used, art. 416-bis relies on the intimidatory effect resulting from the mafia-method, which instead is missing in the simple unlawful association under art. 416. Therefore, a mafia-type association requires also a relevant intimidatory power on the territory.

As per the goal, the difference between articles relies on the criminal plan. Mafia-type associations do not necessarily aim to perpetrate specific crimes (while art. 416 recalls the intention to perpetrate several offences) and may achieve unlawful profits or advantages, for themself or other parties, by using the mafia-method. Therefore, art. 416-bis has a much broader scope of application than a simple unlawful association.

Subjective element of the crime

The subjective element is represented by the specific fraudulent intention to knowingly participate to the conspiracy and be available to act, with any relevant conduct, in order to preserve or strengthen the association and achieve common goals.

According to a minor doctrinal view, the subjective element may require a generic fraudulent intention to join the association and be aware of the goal and means used by the conspiracy.

Perpetration of the offence

According to the Supreme Courte the crime "*is perpetrated by a single member, when a subject provides a minimum contribution to the association, which is considered as necessary to qualify its membership*".

Considerations to identify offences with administrative liability relevant for art. 24-ter of the Decree

Doctrine questioned several times whether, pursuant to art. 24-ter of the Decree, the unlawful association is relevant only if one of the offences of the Decree is perpetrated or, instead, any kind of crime (including criminal and special laws) may occur, even though not included in the Decree.

Far from having a common view of this topic, the issue is extremely relevant, especially from the implementation perspective, as it has deep impact when mapping sensitive activities to set up the organisational, management and control model.

a) Extensive approach

According to several authors, it may be feasible to charge an entity with administrative liability arising from offences not included in the Decree, although relevant from the unlawful association perspective. In other words, pursuant to D. Lgs. no. 231/01, the entity may be liable of offences perpetrated by unlawful association (e.g. tax or corporate crimes), while the same offences, perpetrated by an individual, may not result in administrative liability.

However this approach causes several issues to assess risks for the Model 231. In particular, by including any type of crimes perpetrated by the conspiracy, it would be extremely difficult, if not impossible, to map any kind of risk.

Notwithstanding the commitment to consolidate such approach, no analysis may ensure a full risk management in relation to all possible offences. Supporters of such approach criticised the intention of the Legislator when introduced a hypothetical administrative liability for the entity when, at the same time, it is not feasible to implement effective prevention protocols.

b) Restrictive approach

According to this doctrine, it is not feasible to charge an entity with administrative liability arising from offences not included in the Decree, although relevant from the unlawful association perspective. Therefore, art. 24-ter of the Decree may be applied to unlawful association as long as the offence is set forth by D. Lgs. no. 231/01,

The basis of such approach relies on the principle of legality introduced by art. 2 of D. Lgs. no. 231/01, which states: "*Entities may not be liable for acts constituting offences if their administrative liability regarding such offences and related sanctions is not expressly contemplated under a law coming into force prior to the date on which the offence is committed*".

c) Final thoughts

Given the current doctrinal debate mentioned earlier and on the basis of the aforementioned principle of legality, the Company adopted the restrictive approach by focusing on the offences relevant and potentially applicable within the Company. This is a consequence of the critical issues potentially arising during risk mapping, when the extensive approach is applied.

With reference to the offences under art. 24-ter of the Decree and art. 10 of Law no. 146/2006, the majority of the crimes are unrelated to SNAITECH business and totally against its values and principles.

In particular with reference to: kidnapping for ransom; conspiracy to unlawfully engage in the traffic of narcotic and psychotropic substances; illegal manufacturing, of weapons; illegal immigration; smuggling of foreign tobacco products.

Different considerations apply on unlawful association to commit a crime as per art. 416 of C.P., which relies on the stability and continuity of the association and its intention to perpetrate an undetermined number of crimes.

In this circumstance, it shall be assessed the risk that several employees may use the organisational structure of SNAITECH to perpetrate several crimes for the benefit of the same company (often addressed to art. 416 of C.P. by the jurisprudence).

The risk is therefore linked to the attitudes and intentions of some SNAITECH employees to use the organisation with the aim to perpetrate criminal activities.

The only prevention measure applicable is the broadest disclosure of the Company's attitude and business philosophy by stating that:

- ✓ *It is never allowed to achieve profits or benefits in the company's interest through illegal activities;*

- ✓ *The company shall adopt any measure to ensure a prompt return to legality and transparency in a specific division, if there is reasonable ground to believe that several individuals are perpetrating criminal offences, also in the interest of company.*

Same considerations apply to the mafia-type association and bargaining of votes.

The former is totally opposed to SNAITECH purposes. However, to avoid any remote risks of employees diverging from their conducts, it was recalled the basic principles and free competition rules followed by SNAITECH and imposed to all its stakeholders.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal;
- Business support;
- Occupational safety and health;
- IT;
- Administration, Finance and Audit;
- Marketing and communication;
- Compliance;
- Procurement of goods and services;
- HR.

4. Sensitive activities related to organised crime and transnational offences

Crimes under art. 24-ter of Decree and art. 10 of Law no. 146/2006 are not easily linkable to the business and activities performed by the Company. Furthermore:

- Such crimes are mainly perpetrated by associations (unlawful association, mafia-type association) or mainly connect to associations (bargaining of votes, crimes perpetrated with the mafia-method) and, therefore, any agreement between individuals aimed at perpetrating an undetermined number of crimes is punished accordingly;

- Crimes of association include an undetermined number of offences, which may be perpetrated during any type of activity performed by the Company.

Despite such crimes are not easily linkable to the business and activities performed by the Company – and therefore its relevant operating procedure – such crimes may be perpetrated either by the management and employees. It is therefore of extreme relevance the prevention system implemented by the Company.

Indeed, the corporate governance controls, principles of the Ethical Code and prevention protocols included in the Special Sections (A, B, C, D, E, F, G, H, I, L, M, N, O and P) may be effective prevention tools against the offences. They may represent the most suitable tool against the offence of unlawful association under art. 416 of C.P., given the difficulty to prevent potentially infinite crimes.

The Company has anyway identified a list of activities where conspirators may interact with the Company. In particular, the following list includes all sensitive activities potentially exposed to perpetration of offences related to organised crime (art. 24-ter of Decree) and transnational crimes (art. 10 of Law no. 146/2006):

- ✓ Screening and selection of agents;
- ✓ Management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;
- ✓ Management of relations with clients/partners in the retail space (gaming machine owners, retailers, independent associations, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;
- ✓ Management of relations with final customers, including set up of minimum requirements, due diligence, qualifications, screening and management of contractual agreement and finalisation of the gambling account;
- ✓ Acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events);
- ✓ Management of the procedures for the procurement of goods and services (including screening of suppliers);
- ✓ Management of the procedures for the appointment of professional consultants (including screening and other relations (also of legal nature) with consultants);
- ✓ Treasury activities including cash movements of bank accounts;
- ✓ Screening, hiring and management of personnel (also indirectly through third parties);
- ✓ Management of intragroup relations and duties (Investments, Contracts, information flows, etc.);
- ✓ Management of horseraces (including horse hosting, controls of documentation, enrolment to competitions, etc.);
- ✓ Management of residual betting and relations with bookmakers at the end of the horseracing event, including storage of *borderau* and update of MIPAAF account;
- ✓ Management of real estate assets rented to horserace operators (e.g. restaurant, clinic, golf, etc.).

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Specific prevention protocols

For transactions related to the **screening and selection of agents**, provisions of par. 5 of Special Section A – Offences against the Public Administration – apply in relation to the sensitive activities.

For transactions related to: **management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement; management of the procedures for the procurement of goods and services (including screening of suppliers); management of the procedures for the appointment of professional consultants (including screening and other relations (also of legal nature) with consultants)**. The provisions of par. 6 of Special Section E – Offences related to handling stolen goods, laundering and self-laundering, use of money, assets or benefits of illegal origin – apply in relation to the sensitive activities. Furthermore, protocols require that any invoice of goods or services purchased shall be checked (existence and amount) against relevant contracts, purchase orders and confirmations.

For transactions related to: **management of relations with clients/partners in the retail space (gaming machine owners, retailers, independent associations, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement; management of relations with final customers, including set up of minimum requirements, due diligence, qualifications, screening and management of contractual agreement and finalisation of the gambling account; management of real estate assets rented to horserace operators (e.g. restaurant, clinic, golf, etc.)**. Protocols shall include the following steps:

- ✓ Screening and selection of third parties shall always be compliant with relevant applicable anti-mafia laws;
- ✓ Any purchase of goods and services is ruled by contracts or written orders with precise indications of prices and relevant criteria to assess it;
- ✓ Contracts related to the supply of goods and services shall include specific clauses and liabilities to comply with contractual obligations and shall adhere to the principles of Ethical Code and Model.

For transactions related to: **acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events); treasury activities including cash movements of bank accounts**. The provisions of par. 6 of Special Section E – Offences related to handling stolen goods, laundering and self-laundering, use of money, assets or benefits of illegal origin – apply in relation to the sensitive activities.

For transactions related to **screening, hiring and management of personnel (also indirectly through third parties)**, provisions of par. 5 of Special Section A – Offences against the Public Administration – apply in relation to the sensitive activities.

For transactions related to the **management of intragroup relations and duties (Investments, Contracts, information flows, etc.)**, provisions of par. 5 of Special Section B – Corporate Offences– apply in relation to the sensitive activities.

For transactions related to the **management of horseraces (including hosting of horses, controls of documentation, enrolment to competitions, etc.)**, protocols shall include the following steps:

- ✓ The Company shall not finance, directly or indirectly, subjects whose intention is to perpetrate offences related to organised crime;
- ✓ Set up procedure with roles, activities, duties and controls on horse hosting;
- ✓ Segregation of duties between subject who sets contract values and approve horse hosting contracts;
- ✓ Contracts related to the supply of goods and services shall include specific clauses and liabilities to comply with contractual obligations and shall adhere to the principles of Ethical Code and Model;
- ✓ Matching credit invoices with horse hosting contracts.

For transactions related to the **management of residual betting and relations with bookmakers at the end of the horseracing event, including storage of *borderau* and update of MIPAAF account**, the provisions of par. 6 of Special Section E – Offences related to handling stolen goods, laundering and self-laundering, use of money, assets or benefits of illegal origin – apply in relation to the sensitive activities. Furthermore, protocols identify criteria to assess personal profile of counterparties (criminal convictions; doubtful reputation; direct statements to be involved in criminal activities).

6. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

D.LGS. N. 231/2001

Special Section H

Crimes against Industry and Trade
(Art. 25-bis. 1 of D. Lgs. no. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Offences under art. 25 bis. 1 of D. Lgs no. 231/2001

The current Special Section refers to the offences set forth by art. 25-bis.1 of D. Lgs. no. 231/2001, introduced by Law no. 99 of 23 July 2009, and aims to prevent any commercial and industrial fraud ("Crimes against industry and trade").

A list of offences and related articles of the Criminal Law is disclosed in the following pages:

(i) Undermined freedom of trade and commerce (art. 513 of C.P.)

"Anyone who exercises violence against property or uses fraudulent means to prevent or disrupt the operation of an industry or commerce, unless a more serious offence is committed, is punished with a prison sentence up to two years and a fine from Euro 103 to 1,032 Euro".

(ii) Illegal competition with threats or violence (art. 513-bis of C.P.)

"Anyone who competes using violence or threats when performing commercial, industrial or other activities is punished with a prison sentence from two to six years.

The sanction is increased if the competition relates to activities funded, in full or in part, by the State or other public entities".

(iii) Fraud against national Industries (art. 514 of C.P.)

"Anyone who sells or distributes, in national and foreign markets, industrial products with counterfeited trademarks, names, labels or distinctive marks and causes a damage to the whole national industry, is punished with prison sentence from one to five years and a fine above Euro 516.

If trademarks or distinctive marks were compliant with national laws or international conventions on industrial patents protection, the sanction is increased and the provisions of art. 473 and 474 of c.p. do not apply".

(iv) Commercial fraud (art. 515 c.p.)

"When performing a commercial activity, anyone who delivers goods other than those agreed, or delivers goods which, while being of the same species as the agreed upon goods, differ from them as to origin, provenance, quality or quantity, is punished, unless a major offence apply, with a prison sentence up to two years and a fine up to Euro 2,065.

When trade relates to precious metals, the sanction is increased up to three years with a fine not lower than 103 Euro".

(v) Sale of non-genuine foodstuffs as genuine (art. 516 of C.P.)

"Anyone who sells or distributes non-genuine foodstuffs as genuine is punished with a prison sentence up to six months and a fine of Euro 1,032".

(vi) Sale of industrial products with misleading marks (art. 517 of C.P.)

"Anyone who sells or distributes intellectual works or industrial products with names, trademarks or distinctive marks likely to mislead the buyer about the origin, source or quality of the work or product, is punished, unless a different offence applies, with a prison sentence up to two years and a fine up to 20,000 Euro".

(vii) Manufacture and sale of goods made by infringement industrial property rights (art. 517-ter of C.P.)

"Unless art. 473 and 474 of c.p. apply, any person, potently aware of patents or registrations held by other parties, manufactures or uses for manufacturing purposes items or other goods thereby usurping or violating an industrial property right, is punished, upon compliant of the offended party, with a prison sentence up to two years and a fine up to 20,000 Euro.

The same sanction applies to anyone who, in order to make a profit, introduces in State's territory, holds for sale, sells or otherwise distributes goods described in paragraph 1.

Provisions of art. 474-bis, par. 2 of art. 474-ter and par. 2 of art. 517-bis apply.

Offences under paragraphs 1 and 2 are punished as long as there is compliance with national laws, EU regulations and international conventions on industrial or intellectual patents protection".

(viii) Counterfeiting of geographical indications or denominations of origin of agricultural food products (art. 517-*quater* of C.P.)

"Anyone who counterfeits or alters geographical indications or designations of origin of agricultural food products is punished with prison sentence up to two years and a fine up to Euro 20,000.

The same sanction applies to anyone who, in order to make a profit, introduces in Italy, holds for sale, sells directly to consumers or distributes these products with counterfeit indications or designations.

Provisions of art. 474-bis, par. 2 of art. 474-ter and par. 2 of art. 517-bis apply.

Offences under paragraphs 1 and 2 are punished as long as there is compliance with national laws, EU regulations and international conventions on geographical indications and denominations of origin of agricultural food products".

On the basis of the activities performed by SNAITECH S.p.A., the Company has identified the following relevant offence:

- ***Undermined freedom of trade and commerce (art. 513 of C.P.)***

The offence is perpetrated through an economic aggression by using violence against property or fraudulent means to prevent or disrupt the operation of an industry or commerce.

The provision aims to preserve the freedom of economic activities of citizens.

The offence covers the two following alternative conducts:

- Using violence against property which implies damaging, transformation or changing its use;

- Using fraudulent means such as artifices, scams and lies to mislead the victims, including for example the use of someone's trademarks, disclosure of fake news or advertisement and parasitic competition.

The offence is perpetrated, from a subjective perspective, if there is awareness and willingness of the conduct along with the aim to prevent or disrupt.

For example, the offence may be perpetrated if SNAITECH alters the integrity of online gambling parameters with the aim to alter gambling functioning.

2. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Business support;
- Compliance;
- Procurement of goods and services

3. Sensitive activities related to crimes against industry and trade

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to crimes against industry and trade, pursuant to articles 25-bis.1 of the Decree:

- ✓ Management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;

- ✓ Management and assessment of the integrity of gambling parameters and proper functioning and use of gambling (in compliance with ADM regulation).

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

4. Specific prevention protocols

For transactions related to the **management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement**, protocols shall include the following steps:

- ✓ When selecting a supplier, preliminary controls shall be conducted to assess and monitor technical, organisational and managerial skills as well as ethical, economical and financial reliability;
- ✓ Newly selected suppliers shall be subject to specific process aimed at assessing quality and technical details of goods received against quality and technical standards stated by the suppliers;
- ✓ Contracts with suppliers shall include specific clauses:
  - To match characteristics of goods provided against the ones included in the contracts;
  - Indemnities for any breach of third parties' right by suppliers and related to the goods provided;
- ✓ Any use of third parties' trademark shall be duly authorised and licensed;
- ✓ Set up controls to assess compliance of goods purchased with technical standards stated by the supplier.

For transactions related to the **management and assessment of the integrity of gambling parameters and proper functioning and use of gambling (in compliance with ADM regulation)**, protocols shall include the following steps:

- ✓ There is segregation of duties between the subject who manage and assess the integrity of gambling parameters;
- ✓ Ensure fairness and transparency when managing and assessing the integrity of gambling parameters;
- ✓ No actions shall be taken to alter functioning and use of gambling;
- ✓ Set up training programs for employees on prevention of crimes against industry and trade.

5. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated

6. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D. LGS. NO. 231/01

Special Section I

Offences related to copyright infringement
(Art. 25 novies of D.Lgs. no. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Offences under art. 25-*novies* of D.Lgs. no. 231/2001

Offences related to copyright infringement were introduced by the Special Law no. 633/1941 (and subsequent additions/amendments) and recalled by D. Lgs. no. 231/01 (through the Law no.99/2009).

According to the Law no. 633/1941 "**Protection of copyright and neighbouring rights**":

***Making available, in telecommunications networks, protected intellectual works without authorisation (*art 171 – par. 1 lett. a-bis)**

"Without prejudice to art. 171-bis and 171-ter, it is punished with a fine from Euro 51 to Euro 2,065, any person who, without being authorised, for any purpose and in any form, makes available to the public a protected intellectual work, or a part thereof, by disseminating it in any kind of telecommunication systems".

***Aggravated unauthorised use of protected intellectual works* (art 171 – par. 3)**

"Prison sentence up to one year and a fine not lower than Euro 516 apply when the aforementioned crimes are perpetrated if there is a prohibition of publication imposed by the author, or by usurping authorship (plagiarism), or by deforming, altering or otherwise changing the work in a way that harms the author's honour or reputation".

***Abuses concerning software and databases* (art 171-bis, par. 1)**

"Anyone who unlawfully duplicates, with the aim to gain profits, computer software or imports, distributes, sells, holds for commercial or business purposes or leases computer software unlabelled with SIAE mark (Italian Association of Authors and Publishers) is punished with a prison sentence from six months to three years and a fine from Euro 2,582 to Euro 15,493.

Same sanctions apply to person who prepares, holds or exchanges any means aimed at removing or circumventing software protection devices. Prison sentence may not be lower than two years with a fine of Euro 15,493 for serious conducts".

***Abuses concerning software and databases (*Art 171-bis, par. 2)**

"Anyone who, with the aim to gain profits, duplicates, transfers on other devices, distributes, communicates, discloses to the public content of a database, using other devices unlabelled with SIAE mark, in breach of art. 64-quinquies and 64-sexies, or retrieves, re-uses the database in breach of art. 102-bis and 102-ter, or distributes, sells or leases a database, is punished with a prison sentence from six months to three years and a fine from Euro 2,582 to Euro 15,493. Prison sentence may not be lower than two years with a fine of Euro 15,493 for serious conducts".

*Abuses concerning audio-visual or literary works (*art. 171-ter)

"If the offence is committed for non-personal use and for profit-making purposes, prison sentence from six months to three years and a fine from Euro 2,582 to Euro 15,493 apply to anyone who:

a) unlawfully duplicates or reproduces works intended for cinematographic or television distribution, records, tapes or other media containing audio clip or video clip of musical, film or similar audio-visual works or sequences of moving images;
b) unlawfully duplicates, reproduces, disseminates to the public, with any means, in full or in part, literacy, dramatic, scientific or educational work, musical or musical drama works or multimedia works;
c) albeit not involved in the unauthorised duplication or reproduction, introduces in Italy, holds for sale or distribution, sells, supplies, shows in public or broadcasts on television or radio, or plays in public the unauthorised copies or reproductions under letter a) and b);
d) sells or leases videotapes, music tapes or any other media containing phonograms or video grams of cinematographic or audio-visual works unlabelled with SIAE mark, pursuant to the current law;
e) without specific agreement with the legitimate broadcaster, disseminates, with any means, services provided with unscramblers of encrypted transmissions;
f) introduces in the State's territory, holds for sales or distribution, distributes, sells, leases, promotes, installs devices which enable unauthorised access to such services or products aimed at circumventing the technology safeguards preventing unauthorised uses of protected works;

f-bis) manufactures, distributes, sells, leases, promotes for sale or lease, holds for commercial purposes any device or services aimed at circumventing technology safeguards set forth by art. 102-quater.

h) removes or alters electronic copyright notices set forth by art. 102-quiquies or distributes, imports for subsequent distribution, disseminates on radio or television, discloses to the public works from which the above-mentioned copyright information has been deleted or altered.

It is punished with prison sentence from one to four years and a fine from Euro 2,582 to Euro 15,493 anyone who:

a) unlawfully duplicates, transfers on other devices, distributes, sells or imports, more than fifty copies of works protected by copyrights;

a-bis) in breach of art. 16, makes available to the public a protected intellectual work, or a part thereof, by disseminating it in any kind of telecommunication systems;

b) performing regularly business activities related to duplication, distribution, sale, promotion or import of protected intellectual work, is chargeable with offences under par. 1;

c) promotes or organised the unlawful activities under par. 1;

Sanction is reduced for minor offences.

Sanctions applicable to offences in par. 1 include:

a) ancillary sanctions of art. 30 and 32-bis of criminal law;

b) publication of the sentence in one more national newspapers and in one or more specialized magazines.

c) suspension for one year of broadcasting concession or authorisation.

The amounts from the application of the fines included in previous paragraphs shall be paid to the National Providence and Assistance Agency for Painters and Sculptors, Musicians, Writers and Playwrights".

Failure to make communications or making false communications to SIAE ((art. 171-septies)

"Sanction under par. 1, art. 171-ter applies also to:

a) manufacturers or importers of media containing software intended for sale who fail to provide SIAE with the data necessary to identify the media in respect of which they wish to avail themselves of exemption from the obligation to affix the SIAE mark;

b) unless a major offence applies, anyone who provides false statement of compliance with legal obligation under par. 2, art. 181-bis of the current law".

Fraudulent unscrambling of restricted-access transmissions (art 171-octies)

"Unless a major offence applies, it is punished with a prison sentence from six months to three years and a fine from Euro 2,582 to Euro 25,822, anyone who with fraudulent purposes, produces, imports, distributes, installs, sells, modifies or uses, also for personal use only, devices for unscrambling restricted access video transmissions, also where these are receivable free of charge. For major offences the prison sentence may not be lower than two years with a fine of Euro15,493".

Given the activities performed by SNAITECH, all the offences under art. 25-novies of the Decree are of relevant nature.

2. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- IT;
- Business support;
- Compliance;
- Procurement of goods and services.

3. Sensitive activities related to copyright infringement

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to copyright infringement, pursuant to article 25-novies of the Decree:

- ✓ Purchase, development and maintenance of information systems;
- ✓ Instalments, management and usage of software, graphics, images without any licence and authorisation or playing and disseminating in PoS any multimedia content, which is illegal, counterfeit or missing payment contribution to SIAE.

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

4. Specific prevention protocols

For transactions related to: **purchase, development and maintenance of information systems; instalments, management and usage of software, graphics, images without any licence and authorisation or playing and disseminating in PoS any multimedia content, which is illegal, counterfeit or missing payment contribution to SIAE**. Protocols shall include the following steps:

- ✓ Sep up criteria and procedures to manage software and update related inventory;
- ✓ The Company shall ensure, with relevant authorisation, that images used for ads are freely usable;
- ✓ The Company may use any content related to software, graphics, images under proper authorisation and license only;
- ✓ Set up criteria and procedures to control purchase and use of any software duly certified and authorised; furthermore, it shall be periodically verified the existence of any prohibited and/or unauthorised software loaded on computers of the Company;
- ✓ Documentation related to any activity shall be stored in order to ensure full traceability;
- ✓ Application shall track any change of data and systems made by users;
- ✓ Set up procedures to claim any reimbursement to SIAE related to private copies;
- ✓ Any copyright work purchased by the Company for communication and/or marketing purposes shall be listed in specific database;
- ✓ When purchasing licensed works, database shall include the following data:
  - Purchase date;
  - Expiry date;

- Usage of license contract (e.g. upload on website, dissemination to public, inclusion in brochure and maximum number of copies, etc.);

✓ Set up criteria and procedures to monitor users' access to databases;

✓ Contracts with third parties shall include specific clauses on copyright.

5. Information flows to SB

Persons in charge of relevant functions shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

6. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D.LGS. N. 231/01

Special Section L

Crimes related to counterfeiting of money (and valuables)

(Art. 25 bis of D.Lgs. no. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

The current Special Section refers to the offences set forth by art. 25-bis of Decree and potentially relevant for SNAITECH S.p.A.

In particular, it rules the conduct held by those subjects – directors, managers and employees of SNAITECH as well as collaborators, external advisors and suppliers performing their services within the Company regardless the legal nature of their relationship with the Company – involved in the process and sensitive activities ("Recipients").

All Recipients of the current Special Section of the Model shall behave in compliance with the following provisions, in order to prevent the perpetration of any crime set forth by relevant laws.

2. Crimes under art. 25-bis of D.Lgs. no. 231/2001

Counterfeiting money, spending and introducing counterfeit money into the country, in conspiracy with others (art. 453 of C.P.).

"It is punished with prison sentence from three to twelve years and fine from Euro 516 to Euro 3,098 anyone who:

1. *Counterfeits national or foreign currency;*
2. *alters money such that it appear to have a higher value than the true one*
3. *albeit not involved in counterfeiting or alteration, cooperates with the authors or intermediary by introducing into the State territory, holding or putting into circulation the counterfeited or altered money;*
4. *obtains such counterfeit or altered money, with the aim to distribute it, from either the author of the counterfeiting or alteration or from his intermediary".*

Altering money (art. 454 of C.P.)

"Anyone who alters money identified in previous article and decreases its value or perpetrates any offence listed in n. 3 and 4 of previous article, is punished with prison sentence from one to five years and a fine from Euro 103 to Euro 516."

Spending and introducing counterfeit money into the country, not in conspiracy with others (art. 455 of C.P.)

"Anyone who, outside of offences under previous articles, introduces into the State territory, purchases or holds counterfeited or altered money, with the aim to distribute it, or spends or puts into circulation, is subject to the same sanctions of previous articles, reduced by one third".

Unknowingly passing counterfeit money (art. 457 of C.P.)

"Anyone who spends or puts into circulations counterfeited or altered money, received in good faith, is punished with prison sentence up to six months and a fine of Euro 1,032".

Counterfeiting official stamps, introducing into the country, purchasing, possessing or circulating counterfeit official stamps (art. 459 of C.P.)

"Provisions of art. 453, 455 and 457 apply to counterfeiting or alteration of official stamps and the introduction in the State territory, purchasing, holding or putting into circulation of counterfeited official stamps; sanctions are reduced by one third.

Official stamps include stamped paper, stamps and other similar values".

Counterfeiting of watermarked paper for producing banknotes or official stamps (art. 460 of C.P.)

"Anyone who counterfeits watermarked paper for producing banknotes or official stamps, or purchases, holds or sells it, is punished, unless a major offence applies, with a prison sentence from two to six years and a fine from Euro 309 to Euro 1,032".

Making or possessing watermarks or instruments for the purpose of counterfeiting money, official stamps or of watermarked paper (art. 461 of C.P.)

"Anyone who produces, purchases, holds or sells watermarks, software or devices aimed at counterfeiting or altering money, stamps or watermarked paper, is punished, unless a major offence applies, with a prison sentence from one to five years and a fine from Euro 103 to Euro 516.

Same sanction applies if conducts described in par. 1 refers to hologram or other part of the money ensuring protection against counterfeiting or alteration".

Using counterfeit or altered official stamps (art. 464 of C.P.)

"Anyone who, despite not involved in counterfeiting or alteration, uses counterfeited or altered official stamps is punished with a prison sentence up to three years and a fine up to Euro 516.

If official stamps were received in good faith, then sanction of art. 457 applies reduced by one third".

Counterfeiting, alteration or use of distinctive marks of intellectual works or industrial products (art. 473 of C.P.)

"Any person who, despite being able to ascertain that trademarks and other distinctive marks of industrial products belong to other parties, counterfeits them, or alters the original marks, or uses counterfeit marks without having taken part in their counterfeiting, is punished with prison sentence from six months to three years and a fine from Euro 2,500 to Euro 25,000.

Prison sentence from one to four years and a fine from Euro 3,500 to Euro 35,000 apply to anyone who counterfeits or alters patents, designs and industrial models, national or foreign or uses, without being involved in the counterfeiting, these counterfeited patents, designs or models.

Offences under par. 1 and 2 are punishable as long as there is compliance with internal law, EU regulation and international conventions on protection of intellectual and industrial work".

Introducing into the country and selling products bearing counterfeit marks (art. 474 of C.P.)

"Excluding conducts related to art. 473, anyone who introduces in the State territory, with the aim to gain profits, national or foreign products bearing counterfeited or altered marks or distinctive signs, or holds for sale, sells or puts into circulation such counterfeited products, is punished with a prison sentence from one to four years and a fine from Euro 3,500 to 35,000.

Excluding the involvement in counterfeiting, altering or introducing in the State territory, anyone who holds for sales, sells or puts into circulation, with the aim to gain profits, products described in the first paragraph, is punished with a prison sentence up to two years and a fine up to Euro 20,000.

Offences under par. 1 and 2 are punishable as long as there is compliance with internal law, EU regulation and international conventions on protection of intellectual and industrial work".

In relation to SNAITECH business, the following articles were considered relevant:

i. Counterfeiting money, spending and introducing counterfeit money into the country, in conspiracy with others (art. 453 of C.P.)

The offence is perpetrated when money is counterfeited or altered, introduced in the State territory, purchased or received.

Therefore, criminal liability arises from one of the following alternative conducts: i) counterfeiting national or foreign currency; ii) alteration of money; iii) introduction into the State territory, holding or distributing counterfeited or altered money; iv) obtaining such counterfeit or altered money, with the aim to distribute it.

ii. Spending and introducing counterfeit money into the country, not in conspiracy with others (art. 455 of C.P.)

The offence is perpetrated when altered or counterfeited money are hold or purchased with the aim to distribute it.

From a subjective perspective, the offence requires awareness and willingness by the offender to introduce into the State territory, purchase, hold, spend or distribute counterfeited or altered money, whose real origin are known to the offender.

iii. Unknowingly passing counterfeit money (art. 457 of C.P.)

Spending counterfeited or altered money, received in good faith, constitutes crime if, after having acknowledged counterfeiting, money are spent or distributed.

The criminal liability arises when money is spent or distributed.

Given the frequency and movements of money arising from bets acceptance and winning payment occurred in SNAITECH Point of Sales, the above offences were deemed relevant.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Administration, Finance and Audit;
- Business support;
- Compliance.

4. Sensitive activities related to counterfeiting of money

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to crimes related to counterfeiting of money, pursuant to article 25-bis of the Decree:

- ✓ Acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events);

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Specific prevention protocols

For transactions related to the a**cceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events)**, protocols shall include the following steps:

- ✓ Formal identification of payment methods accepted by PoS;
- ✓ Front-office staff shall be duly informed and trained to identify counterfeited money;
- ✓ Provide PoS with specific devices to detect possible counterfeiting or alterations;
- ✓ Set up procedures to manage potential counterfeited or altered money collected;
- ✓ Produce a summary of cash transactions for PoS (collection and payments);
- ✓ Duty to inform the SB of any concrete or potential distribution of counterfeited or altered money;
- ✓ Once counterfeiting is detected, counterfeited money shall be promptly withdrawn in compliance with current laws and provisions of the Model;

- ✓ In the event of concrete or potential counterfeiting or alteration, money shall be sent to Bank of Italy by filing relevant forms set by current regulations;
- ✓ The person in charge of the relevant Function shall store any documentation such that any further amendment is allowed only with specific authorisation and relevant evidence is provided (in order to ensure proper traceability of the process and facilitate any eventual subsequent control).
- ✓ The Company shall prohibits to: i) make cash payments but minor economic transactions and winnings up to the maximum value allowed by regulation; ii) alter money; iii) use money without having performed relevant counterfeiting controls;
- ✓ All recipients of the model are prohibited to: i) behave such that a potential offence may be perpetrated; ii) implement or facilitate activities not compliant with the Ethical Code; iii) implement activities against principles required by prevention of counterfeiting of money;
- ✓ All the activities and transactions shall comply with current laws and principles of fairness, transparency and good faith;
- ✓ Full matching between actual behaviours and conducts required by internal procedures, especially in relation to sensitive activities;
- ✓ Persons in charge of control and supervision of sensitive activities shall comply with relevant duties and promptly inform the SB of any anomaly.

6. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D. LGS. NO.231/01

Special Section M

Inducements not to give statements or to give untruthful statements before the judicial authorities

SNAITECH S.p.A.

SPECIAL SECTION M – INDUCEMENT NOT TO GIVE OR TO GIVE UNTRUTHFUL STATEMENTS BEFORE THE JUDICIAL AUTHORITIES

TABLE OF CONTENTS

1. Offences under art. 25 - decies of D. Lgs. no. 231/2001

Art. 4 of law no. 116, dated 3 August 2009, "Ratification and execution of the United Nations Convention against Corruption, adopted by the UN General Assembly on 31October 2003 with Resolution no. 58/4, signed by the Italian State on 9 December 2003, and the internal implementation provisions and amendments to the Criminal Law and the Criminal Procedure Law" extended the administrative liability of entities arising from offence set forth by art. 377-bis of C.P., by introducing it into art. 25-decies of the Decree.

An excerpt of the article along with comments is provided herein below:

Inducement not to give statement or to give an untruthful statement before the judicial authority (art. 377-bis of C.P.)

"Unless a major offence is perpetrated, anyone who uses violence or threats, offers or promises money or other benefits to induce not to make statements, or to make false statements any person who is called before the judicial authorities to make statements in connection with criminal proceedings, if such person has the right to remain silent, then is punished with a prison sentence from two to six years".

The offence is perpetrated by anyone who uses violence or threats, or offers or promises money or other benefit to induce not to make statements, or to make false statements any person who is called before the judicial authorities to make statements in connection with criminal proceedings, if such person has the right to remain silent.

The conduct may be addressed to investigated persons or defendants who have the right to remain silent.

Inducement is achieved by influencing psyche of an individual with the aim to force specific conducts or behaviours, also by using violence, threats or promising money or other benefits.

Furthermore, the following requirements apply for this offence:

- Person under inducement did not released any statement or gave untruthful statements;
- Such person had the right to remain silent.

2. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Business support;
- Legal;
- Occupational safety and health;
- IT;

- Administration, Finance and Audit;
- Marketing and communication;
- Compliance;
- Environmental supervision;
- Procurement of goods and services;
- HR.

3. Sensitive activities related to inducement not to give or to give untruthful statements before the judicial authorities

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to crimes set forth by article 25-bis of the Decree:

- ✓ Management of relations with judicial authorities during litigations (fiscal, administrative, civil, labour and appeals against the entity issuing the concession).

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

4. Specific prevention protocols

For transactions related to the **management of relations with judicial authorities during litigations (fiscal, administrative, civil, labour and appeals against the entity issuing the concession)**. Protocols include the following steps:

- ✓ Set up procedures for roles, activities, responsibilities and controls related to relations with financial institutions and intermediaries;
- ✓ Identify subjects with power of representation of the Company to deal with Public Administration during litigations;
- ✓ Identify all relevant subjects authorised to act on behalf of the Company in litigations;
- ✓ There is segregation of duties between subjects who arrange documentation for the relevant Authority and authorise it;
- ✓ All documents to submit to relevant Authorities shall be approved by the Chairman and Chief Executive Officer;
- ✓ Assess pro and cons of any potential action following the notification of a writ of summon;
- ✓ The legal advisor shall be selected according to the following criteria and principles: i) transparency; ii) equal opportunity; iii) professionalism; iv) reliability; v) inexpensiveness;

- ✓ Legal advisors are engaged on written contracts, which must be reviewed and authorised by the Chairman, Chief Executive Officer and Head of Legal and Corporate Affair;
- ✓ Management of the company shall be involved on developing litigation strategies;
- ✓ Management of the company is constantly updated on outstanding litigations;
- ✓ Any contractual relationship with legal advisors is formalised with a mandate letter;
- ✓ The mandate letter or contract shall include specific clauses on the acceptance of the Ethical Code and Model of SNAITECH;
- ✓ All the activities performed by the legal advisors shall be monitored through periodic reports to be stored;
- ✓ Perform controls to: i) monitor pending litigations; ii) assess periodically the completeness and fairness of all requirements related to litigations/transactions;
- ✓ Proceeding shall be tracked, both in terms of information and documents such that: i) each relevant stage shall result from written documents; ii) the relevant division is responsible to store any documentation required by litigation and transactions, in order to retrieve responsibilities and decision taken; iii) the relevant function provides update on current status of litigations to management and relevant divisions.

5. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

6. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

D.LGS. NO. 231/2001

Special Section N

Environmental crimes
(Art. 25-undecies of D. Lgs. no. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

The current Special Section relates to crimes set forth by art. 25-undecies of D. Lgs. no. 231/01 ("**Environmental crimes**"), which are relevant for the administrative liability of the Company.

It is worth highlighting both crimes ruled by the Environment Protection Code and Law no. 68/2015:

- Crimes introduced by the Environment Protection Code relate to the offences caused by fraudulent or negligent conducts; such conducts, in many cases, are considered crimes regardless any damage caused to individuals or environment;

- Law no. 68/0215 has introduced more severe offences, sanctions and investigation tools. The offences mainly require a fraudulent intent, although negligence may apply also to the most severe offences (Environmental pollution and disaster).

2. Offences under art. 25-undecies of D. Lgs. no. 231/01

- **Environmental pollution, disaster, and criminal association with aggravating circumstances regarding the environment (art. 452 - bis, quater, quinquies and octies of C.P.)**

The regulation punishes: all those who unlawfully endanger or bring about a significant and measurable deterioration of water, of air, of the soil or subsoil, of an ecosystem or of the biodiversity; all those who unlawfully provoke an environmental disaster, that consists in the irreversible alteration of the equilibrium of ecosystem, or the elimination of which is particularly burdensome and exceptional, or in harm to public safety based on the severity of the event, the extension or effects, or due to the number of persons harmed or exposed to hazard. The regulation anticipates specific aggravating circumstance for the penalty for crimes of criminal association having the goal of committing any of the environmental offences provided for by the Criminal code. If involving a mafia-type association, the fact itself of acquiring the management or control of an economic activity, of concession, of authorizations, authorizations, public tenders, or of public services regarding environmental matters is an aggravating circumstance.

- **Breach of rules regulating discharges (art. 137, par. 2, 3, 5, 11 and 13 of D. Lgs. no. 152, dated 3 April 2006)**

The offence relates to unauthorised discharges of industrial waste water containing specific hazardous substances, or in contravention of the provisions contained in the authorisation or notwithstanding its suspension or revocation, and discharges of hazardous substances beyond the established limits; breach of discharges restrictions on the ground, in groundwater and underground. Lastly, breach of rules prohibiting discharges into sea of hazardous substances by ships or aircrafts, as defined in international treaties is also punishable, save for authorized discharges of rapidly biodegradable quantities.

- **Breach of waste management regulations (art. 256, par. 1, 3, 5 and 6 of D. Lgs. no. 152, dated 3 April 2006)**

The offence relate to waste collection, transport, retrieval, disposal, sale or brokerage in the absence of the necessary licences, enrolment in the national Register of waste management bodies and notification to the competent authorities or in contravention of provisions included in the licences issued or communicated by the authorities or in the absence of the applicable requirements.

- **Failure to conduct remediation for cases of ground, underground, surface water or groundwater pollution (art. 257, par. 1 and 2 of D. Lgs. no. 152, dated 3 April 2006)**

The offence relates to anyone who brought about the pollution in question, exceeding the risk threshold levels, without informing the competent authority and failing to proceed with site remediation in compliance with projected approved the competent authority.

- **False certification of waste analysis (art. 258, par 4 of D. Lgs. no. 152, dated 3 April 2006)**

Anyone who provides false information on the nature, composition and chemical-physical properties of waste shown on the waste analysis certificate and whosoever utilises a false certificate for the transport of waste is punished accordingly to provision of this article.

- **Illegal shipment of waste (art. 259, par. 1 of D. Lgs. no. 152, dated 3 April 2006)**

The offence is perpetrated by anyone who makes a cross-border shipment of waste in breach of art. 2 of EU Regulation No. 259/1993.

- **Activities organised for the illegal trafficking of waste (art. 260, par. 1 e 2 of D. Lgs. no. 152, dated 3 April 2006)**

Anyone who, with the aim of gain unlawful profits, sells, receives, transports, exports, imports or, in any event, wrongfully manages significant quantities of waste, perpetrates the offence.

- **Substances detrimental to the ozone layer (art. 3, par. 6 of L. no. 549, dated 28 December 1993)**

The offence is perpetrated when conducting unlawful activities related to: trade, use, import, export and retention of substances, which are detrimental to the ozone layer.

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Compliance;
- Occupational safety and health;
- Environmental supervision.

4. Sensitive activities related to Environmental Crimes

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to environmental crimes set forth by art. 25-undecies of the Decree:

- ✓ Management of environmental compliance (e.g. control of environmental regulation, assessment of environmental aspects, documentation, authorisations, monitoring, etc.);
- ✓ Management of operation and documents related to waste cycle: identification of CER code, waste sorting, monitoring temporary dismissal of waste, FIR form, delivery to waste transporters for dismissal/recycling;
- ✓ Management, monitoring and dismissal of asbestos including relevant activities of identification, classification, recording and dismissal;
- ✓ Management of waste water discharge (management of structural intervention on discharge);
- ✓ Management of environmental remediation (management of structural intervention on aquifers, soil, real estate assets, underground tanks, etc.);
- ✓ Management of suppliers: selection and assessment of suppliers providing relevant services (e.g. maintenance, cleaning, etc.);
- ✓ Identification, assessment and management of environmental anomalies, accidents and emergencies, which may endanger the environment, protected areas and public safety;
- ✓ Management of ordinary and extraordinary maintenance;
- ✓ Management of tenders and controls on purchases, documentation and mandatory authorisations.

In relation to those activities, which may involve also public officials or person in charge of public service, it shall apply also Special Section A “Offences against the Public Administration”.

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Prevention protocols

5.1. General prevention protocols

The following general principles apply when managing relevant environmental aspects.

- **Ethical Code**

The Company, through the Ethical Code, is committed to ensure full compliance with relevant environmental laws.

In particular, the Company is committed to:

- ✓ Balance customer satisfaction, public needs and environmental care by relying on processes aimed to exploit professional expertise of employees and responsibilities of management to achieve company goals;

- ✓ Implements strategies aimed at constantly improving environmental protection by focusing on pollution prevention and reduction of environmental risks and impacts.

- **Duties and Responsibilities**

The Company has adopted a formal system of proxies and authorisation for persons in charge of activities with relevant environmental impacts. This system includes:

- ✓ Minimum requirements – to be assessed periodically – for single functions, according to organisational needs and law provisions (e.g. previous experience, specific title, competences and training, etc.);

- ✓ Processes and procedures to describe functions related to relevant activities of the Company.

The Company, following the merger by incorporation of Società Trenno S.r.l., agreed, pursuant to D. Lgs. 152/2006 and subsequently amendment and additions of D. Lgs. 4/2008 and D.M. 6 September 1994, to appoint an Environmental Supervisor in charge of all the functions related to environmental safety of SNAITECH S.p.A. This subject, selected on the basis of professionalism and experience, is in charge of all functions related to compliance and update of relevant environmental regulation.

- **Competences, training and awareness**

The Company implements specific tools to rule information and training processes, also in relation to the environment; in particular, these tools shall include:

- ✓ Duties and responsibilities on environmental training and related procedures (mandatory for all employees);

- ✓ Criteria to update and/or increase training sessions, following relocations, changes, new duties, new equipment or technologies with relevant environmental impact, etc.;

- ✓ Training contents shall be adjusted in accordance with role and duties covered, especially for those functions involved in environmental aspects;

- ✓ Timing to dispense training (e.g. scheduling a training program).

- **Identify environmental aspects and operational control**

The Company establishes criteria and subjects in charge to identify and control sensitive activities in relation to negative environmental impacts in order to:

- ✓ Identify relevant environmental aspects;

- ✓ Determine and assess relevance of negative environmental impacts, which may lead to potential environmental offences;

- ✓ Identify measures to control negative environmental impacts, on the basis of tolerance level previously assessed.

On this purpose, the Company adopted specific procedures aimed at favouring the identification, assessment and control of negative environmental impacts under normal conditions, anomalies and emergency situations.

- **Compliance with current legislation**

In order to comply with current regulation, the Company adopted specific system with:

- ✓ Duties and responsibilities required by relevant environmental regulations and provisions;

- ✓ Criteria and procedures to control regulatory update as well as to report to competent divisions;

- ✓ Criteria and procedures to assess best practices and technical regulation on environmental protection.

- **Management of documentation**

The Company adopted a specific procedure to control all documentation related to the environment. Such procedure includes:

- ✓ Duties and responsibilities to manage documentation (e.g. Manuals, procedures, instructions) in accordance with internal policy;

- ✓ Procedures for recording, managing and storage documentation (e.g. methods to store and protocol documents by ensuring traceability).

- **Audit activities**

In relation to auditing the effectiveness and efficiency of the environmental system, the Company set duties, responsibilities and operational procedures to perform audit activities, including:

✓ Identification and implementation of mitigants;

✓ Reporting auditing results to management.

5.2. Specific prevention protocols

For transactions related to the **management of environmental compliance (e.g. control of environmental regulation, assessment of environmental aspects, documentation, authorisations, monitoring, etc.)**, protocols shall include the following steps:

✓ Procedures to conduct and review the assessment activities of environmental aspects, also in relation to change of organisation, process, plant and anomalies or emergencies;

✓ Procedures to assess environmental requirements of equipment, plan and machinery;

✓ Procedures to identify and monitor all relevant activities required to obtain or renew authorisations;

✓ Duties, responsibilities and procedures to perform audit activities on environmental risks;

✓ Procedures to identify and implement mitigants;

✓ Procedures to disclose results to the relevant functions.

For transactions related to the **management of operation and documents related to waste cycle: identification of CER code, waste sorting, monitoring temporary dismissal of waste, FIR form, delivery to waste transporters for dismissal/recycling**, protocols shall include the following steps:

✓ In relation to waste generation:

- Requirements of products to be purchased shall include also the disposal aspect of the product and, where possible, preference for recycling shall prevail;

- Favour recycling to reduce waste disposal.

✓ In relation to waste collection, the Company shall:

- Determine duties and responsibilities to ensure proper waste classification and identify relevant subjects in charge of the analytical control;

- Ensure proper waste sorting and prevent any illegal mix;

- Ensure proper management of temporary disposal, according to the type and quantity of waste produced;

- Assess any eventual authorisation to collect wastes;
- Schedule and monitor activities as well as report any result to supervisors;
- Ensure availability of relevant documentation (e.g. records of analytical controls).

✓ In relation to waste transfer, the Company shall:

- Set duties and responsibilities to ensure that transporter matches all requirements set by current laws;
- Ensure, if transfer is done by the Company, matching of all requirements set by current laws;
- Ensure full compliance with all requirements of waste transfers (forms, records, etc.);
- Ensure availability of relevant documentation (e.g. records of analytical controls).

✓ In relation to waste disposal, the Company shall:

- Set duties and responsibilities to ensure that subject in charge of disposal matches all requirements set by current laws;
- Ensure full compliance with all requirements of waste disposal;
- Ensure availability of relevant documentation.

For transactions related to the **management, monitoring and dismissal of asbestos including relevant activities of identification, classification, recording and dismissal**, protocols shall include the following steps:

✓ Set criteria to classify materials, according to their nature and storage conditions;

✓ Set criteria to assess properties of materials over time;

✓ Schedule activities for asbestos remediation;

✓ Set temporary measures to manage asbestos (e.g. third parties, additional assessments following deterioration, etc.).

For transactions related to the **management of waste water discharge (management of structural intervention on discharge)**, protocols shall include the following steps:

✓ Set duties and responsibilities to:

- Identify and monitor all relevant activities (affecting the quality of water discharge) required to obtain or renew authorisations;
- Monitor chemical/physical properties of water discharge;
- Periodic maintenance interventions;

- Extraordinary maintenance interventions to limit any environmental accident.

✓ Schedule and ensure, where required, monitoring of chemical/physical properties of water discharge;

✓ Ensure, where required, prompt disclosure of monitoring results to relevant persons in charge;

✓ Ensure availability of relevant documentation (e.g. records of analytical controls).

For transactions related to **management of environmental remediation (management of structural intervention on aquifers, soil, real estate assets, underground tanks, etc.)**, protocols shall include the following steps:

✓ Set up duties and responsibilities to:

- Identify all relevant measure to avoid pollution of soil, subsoil, shallow water and groundwater;

- Ensure periodic maintenance of equipment and plant (e.g. underground tanks or pipes);

- Extraordinary maintenance interventions to limit any environmental accident;

✓ Schedule, if needed, maintenance of wells, shallow water and groundwater to prevent any pollution phenomena;

✓ Establish suitable control measures of any possible pollution;

✓ Set up roles and responsibilities to ensure proper communication in the event of environmental emergency affecting soil, subsoil, shallow water and groundwater;

✓ Ensure availability of relevant documentation (e.g. records of analytical controls);

✓ Schedule and monitor activities and report any result to supervisors;

For transactions related to the **identification, assessment and management of environmental anomalies, accidents and emergencies, which may endanger the environment, protected areas and public safety**, protocols shall include the following steps:

✓ Identify scenarios of possible environmental emergencies;

✓ Determine roles, responsibilities and control measures for emergency situations;

✓ Determine suitable actions to avoid public safety or environmental risks;

✓ Determine timing and procedures of emergency tests;

✓ Determine procedures to record tests, simulations and other emergencies, with the aim to assess suitability of responses and track any action taken.

For transactions related to the **management of suppliers: selection and assessment of suppliers providing relevant services (e.g. maintenance, cleaning, etc.)**, protocols shall include the following steps:

- ✓ Determine criteria to assess critical issues when selecting suppliers;
- ✓ Determine criteria to assess technical and professional requirements when selecting suppliers (e.g. enrolment in specific environmental registers, etc.);
- ✓ Contracts shall include clauses of compliance with current environmental regulation and Company procedures;
- ✓ Determine specific protocols to assess suppliers and their compliance with environmental regulations.

For transactions related to the **management of ordinary and extraordinary maintenance**, protocols shall include the following steps:

- ✓ Set up roles and responsibilities to ensure periodic maintenance interventions (in accordance with manufacturer instruction) on equipment, plant and other assets related to the environment.

For transactions related the **management of tenders and controls on purchases, documentation and mandatory authorisations**, protocols shall include the following steps:

- ✓ Determine procedures to purchase equipment, plant and machinery, including assessment of environmental requirements;
- ✓ Determine, if required, controls on environmental requirements and compliance with current regulation for equipment, plant and machinery (e.g. EC label, etc.);
- ✓ Assess authorisations and certifications;
- ✓ Set up roles and responsibilities to ensure periodic maintenance interventions (in accordance with indication of manufacturers) on equipment, plant and other assets related to the environment.

6. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated.

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D. LGS. NO. 231/01

Special Section O

Employment of immigrants with invalid residence permits (Art. 25- *duodecies* of D.Lgs. no.231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

Art. 25-duodecis of the Decree, introduced by D. Lgs. no. 109, dated 16 July 2012, ("Implementation of the European Directive 2009/52/EC providing for minimum standards on sanctions and measures against employers of illegally staying non-EU nationals") has extended the administrative liability resulting from offences set forth by art. 22, par. 12-bis of D. Lgs. no. 286, dated 25 July 1998.

It relates the offence perpetrated by the employer who hires immigrants without residence permits required by art. 22 of D. Lgs. no. 286, dated 25 July 1998, or with expired permits, or whose permits are withdrawn, if migrants hired are:

- More than three;
- underage;
- exploited or work in breach of violations of the occupational Health and Safety regulations, such as to expose the worker to dangers relating to health, safety or personal security (art. 603-bis, par. 3 of C.P.).

Furthermore, in accordance with Immigration Law, it is punished any person who:

i) "*promotes, manages, organises, finances or transports foreigners into the territory of the State or obtains the illegal entry into other States where the individuals are not citizens or do not have the necessary residence permits*" in accordance with art. 12, par. 3, 3-bis, 3-ter of Immigration Law;

ii) "*in order to obtain an unlawful profit from illegal immigrants or other activities sanctioned by this article, favours immigrants to stay in the State's territory against provisions of this article"* in accordance with art. 12, par. 5 of the Immigration Law.

2. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal;
- Business support;
- Occupational safety and health;
- IT;
- Administration, Finance and Audit;
- Marketing and communication;
- Compliance;
- Procurement of goods and services;
- HR.

3. Sensitive activities related to employment of immigrants with invalid residence permits

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to offences related to employment of immigrants with invalid residence, set forth by art. 25-duodecies of the Decree:

- ✓ Management of terminals instalment and set up (roll-out and connectivity);
- ✓ Management of the procedures for the procurement of goods and services (including screening of suppliers);
- ✓ Screening, hiring and management of personnel (also indirectly through third parties);
- ✓ Ordinary and extraordinary maintenance of horseracing tracks (including premises, equipment, races, green areas, etc.);
- ✓ Screening and selection of suppliers in the environmental field (waste, remediation, etc.).

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

4. Specific prevention protocols

For transactions related to: **management of terminals instalment and set up (roll-out and connectivity); screening, hiring and management of personnel (also indirectly through third parties)**. Protocols shall include the following steps:

- ✓ When hiring non-EU residents, the Company shall rely with relevant authorities to obtain any necessary documentation to legally transfer and hire the prospect employee;
- ✓ When hiring foreign employees based in Italy, the Company shall assess the valid residence or working permit or its renewal;
- ✓ The Company shall support foreign employees to renew working permits and release any relevant documentation or work certification or statement;
- ✓ When the above activities are provided by a third party agency, relation with such agency shall be governed by written contract, which shall include clauses of compliance with the Model and the Decree;
- ✓ The Company adopts a suitable system of proxies and authorisations on topics related to personnel;
- ✓ When the Company relies on workers provided under supply contracts, the relation with the supplier shall be governed by written contract and shall include clauses of compliance with the Model and the Decree.

For transactions related to: **management of the procedures for the procurement of goods and services (including screening of suppliers); ordinary and extraordinary maintenance of horseracing tracks (including premises, equipment, races, green areas, etc.); screening and selection of suppliers in the environmental field (waste, remediation, etc.)**. Protocols shall include the following steps:

- ✓ Assess requirements of counterparty through analysis of relevant documentation required by law (e.g. DURC);

- ✓ Contracts with third parties shall include specific clauses with clear liabilities when incompliant with principles of the Model and Ethical Code. If needed, the contract may impose also certain information duties towards the SB;

- ✓ Contracts with suppliers shall include specific clauses to comply with provisions of work exploitation. In particular, these clauses shall prohibits:

  - To pay, repeatedly, salaries incompliant with the most relevant national collective bargaining agreements and in any case not proportional to the quantity and quality of duties performed by the employees;

  - To breach, repeatedly, regulations on working time, breaks, holidays;

  - To act or breach occupational safety and health regulation.

- ✓ To assess compliance with clauses mentioned above, where possible, the contract shall allow the Company to periodically run inspections of suppliers' premises or request any type of useful documentation;

- ✓ Contracts with suppliers shall also allow the Company to terminate or apply penalties, if one of the above mentioned breaches is detected.

5. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated

6. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL
D. LGS. NO. 231/01

Special Section P

Crimes for purposes of terrorism or designed to subvert democracy
(Art. 25-*quater* of D.Lgs. no. 231/2001)

SNAITECH S.p.A.

TABLE OF CONTENTS

1. Premise

Art. 25-quarter of the Decree does not list specifically crimes while it refers, on the first paragraph, to crimes set forth by criminal law and special laws on terrorism and subversion of democracy, and on the third paragraph, to other crimes against art. 2 of New York convention.

2. Crimes under art. 25-*quater* of D.Lgs. no. 231/2001

This chapter provides an excerpt of relevant articles of criminal law and special laws on terrorism and subversion of democracy, which are deemed relevant for administrative liability of entities, as per article 25-quarter of the Decree.

- **Subversive associations (art. 270 of C.P.)**

"*Anyone who, within the State territory, promotes, established, organises or leads associations aimed at violently establishing a dictatorship of one social class on the other classes or at violently suppressing a social class or violently subverting the economic and social systems of the State, is punished with a prison sentence from five to ten years.*

Anyone who joins the associations ruled under first paragraph is punished with a prison sentence from one to three years.

Sanctions are increased for those who re-establish, including under a false name or fake form, the above-mentioned associations whose dissolution has been ordered".

The offence is perpetrated when a subject promotes, established, organises or leads associations aimed at violently establishing a dictatorship of one social class on the other classes or at violently suppressing a social class or violently subverting the economic and social systems of the State.

- **Associations for terrorist ends including international or for subversion of the democratic order (art. 270-bis of C.P.)**

"*Anyone who promotes, sets up, organizes, manages or finances associations whose purpose is to commit acts of violence for terrorist ends or for subversion of the democratic order is punished with a prison sentence from seven to fifteen years.*

Whoever takes part in any such association is liable to imprisonment of five to ten years.

For the purpose of the criminal law, terrorist ends occur also when the acts of violence are directed against a foreign country, institution or international organization.

For the person condemned it is always obligatory to confiscate those items that serve or were destined for the commission of the crime and items that are the price, product, profit thereof or that comprise their use".

The offence is perpetrated by anyone who promotes, sets up, organizes, manages or finances associations whose purpose is to commit acts of violence for terrorist ends or for subversion of the democratic order. For the purpose of the criminal law, terrorist ends occur also when the acts of violence are directed against a foreign country, institution or international organization.

- **Assisting members (art. 270-ter of C.P.)**

"Anyone who, apart from cases of complicity in the crime or aiding and abetting, gives shelter, food, hospitality, means of transport or communication to participants in the associations mentioned under Articles 270 and 270-bis is liable to imprisonment for up to four years.

The punishment is increased if the assistance given is continuous.

Those who commit the fact in favour of a close relative are not subject to punishment".

The offence is perpetrated by anyone who, apart from cases of complicity in the crime or aiding and abetting, gives shelter, food, hospitality, means of transport or communication to participants in the associations mentioned under Articles 270 and 270-bis

Those who commit the fact in favour of a close relative are not subject to punishment.

- **Recruiting for terrorist ends, including international terrorism) (art. 270-quater of C.P.)**

"Anyone who, except for the cases mentioned under Article 270-bis, trains or otherwise gives instructions on how to prepare or use explosive materials, firearms, or other weapons, harmful or hazardous chemical or bacteriological substances, and all other techniques or methods to commit acts of violence or sabotage of essential public services for the purposes of terrorism, even if directed against a foreign State, an international institution or organization, is punished with a prison sentence from seven to fifteen years.

Except for the cases mentioned under Article 270-bis and in case of training, the recruited person is punished with a prison sentence from five to eight years".

The offence is perpetrated by anyone who, except for the cases mentioned under Article 270-bis, trains or otherwise gives instructions to commit acts of violence or sabotage of essential public services for the purposes of terrorism, even if directed against a foreign State, an international institution or organization.

- **Training for acts of terrorism, including international terrorism (art. 270-quinquies of C.P.)**

"Anyone who, except for the cases mentioned under Article 270-bis, trains or otherwise gives instructions on how to prepare or use explosive materials, firearms, or other weapons, harmful or hazardous chemical or bacteriological substances, and all other techniques or methods to commit acts of violence or sabotage of essential public services for the purposes of terrorism, even if directed against a foreign State, an international institution or organization, is punished with prison sentence from five to ten years.

Same sanctions apply to recruited person or other person who, autonomously acquired instructions on how to prepare acts under first paragraph, perpetrates conducts related to crimes under art. 270-sexies.

Sanctions are increased if training or instruction are dispensed via electronic or telecommunication devices".

The offence is perpetrated by anyone who, except for the cases mentioned under Article 270-bis, trains or otherwise gives instructions on how to prepare or use explosive materials, firearms, or other weapons, harmful or hazardous chemical or bacteriological substances, and all other techniques or methods to commit acts of violence or sabotage of essential public services for the purposes of terrorism, even if directed against a foreign State, an international institution or organization.

- **Financing terrorist activities (art. 270-quinquies. 1 of c.P.)**

"Anyone who, except for the cases mentioned under art. 270-bis and 270-quarter.1, collects, provides or makes available money or other assets, of any origin, to be used for acts of terrorisms as per art. 270-sexies, is punished with a prison sentence from seven to fifteen years, regardless any concrete use of funds to perpetrate the offences.

Anyone who store money or assets mentioned in the first paragraph is punished with prison sentence from five to ten years".

The offence is perpetrated by anyone who, except for the cases mentioned under art. 270-bis and 270-quarter.1, collects, provides or makes available money or other assets, of any origin, to be used for acts of terrorisms as per art. 270-sexies.

- **Embezzlement of confiscated assets or money (art. 270-quinquies. 2 of C.P.)**

"Anyone who embezzles, destroys, loses, deteriorates money or assets, which were confiscated to prevent financing of terrorist activities mentioned in art. 270-sexies, is punished with prison sentence from two to six years and a fine from Euro 3,000 to 15,000".

The offence is perpetrated by anyone who embezzles, destroys, loses, deteriorates money or assets, which were confiscated to prevent financing of terrorist activities mentioned in art. 270-sexies.

- **Acts committed for terrorist purposes (art. 270-sexies of C.P.)**

"Acts committed for terrorist purposes include acts which, by nature or because of their context, can cause serious harm to a country or international organization and are committed in order to intimidate people or coerce public authorities or an international organization to perform, or refrain from performing, any act or to destabilize or destroy the fundamental political, constitutional, economic and social structures of a country or international organization, as well as the other types of terrorist conduct or carried out for terrorist purposes as provided for by conventions or other international laws binding on Italy".

Acts committed for terrorist purposes include acts which, by nature or because of their context, can cause serious harm to a country or international organization and are committed in order to intimidate people or coerce public authorities or an international organization to perform, or refrain from performing, any act or to destabilize or destroy the fundamental political, constitutional, economic and social structures of a country or international organization, as well as the other types of terrorist conduct or carried out for terrorist purposes as provided for by conventions or other international laws binding on Italy

- **Attacks for terrorist or subversive purposes (art. 280 of C.P.)**

"Anyone who, for purposes of terrorism or subverting democracy, attempts against the life or safety of another person is punished, in the former case, with a prison sentence not lower than twenty years, and in the latter case, with a prison sentence not lower than six years.

If the attempt against the safety of any person causes an extremely serious injury, the prison sentence may not be lower than eighteen years; in case of serious injury, the prison sentence may not be lower than twelve years.

If the action is addressed against persons exercising functions in the judicial or prison field or exercising law enforcement functions, sanctions are increased by one third.

If the attempt causes the death of the person, life prison sentence applies if the attempt is against the life; prison sentence of thirty years applies if the attempt is against safety.

Mitigating circumstances, other than ones under art. 98 and 114, along with aggravating circumstances under first and fourth paragraphs, may not be considered equivalent or prevailing and any reduction may apply only where aggravating circumstances applied".

The offence is perpetrated by anyone who, for purposes of terrorism or subverting democracy, attempts against the life or safety of another person.

The offence is more serious if the attempt against the safety of any person causes a serious injury or death or, if the action is addressed against persons exercising functions in the judicial or prison field or exercising law enforcement functions.

- **Terrorist act with lethal or explosive devices (art. 280-bis of C.P.)**

"Unless a major crime applies, anyone who, for terrorist purposes, carries out any acts aimed at damaging tangible or intangible property belonging to another person, through the use of lethal or explosive devices, is punished with a prison sentence from two to five years.

For the current articles, lethal or explosive devices includes weapons or materials listed by art. 585 and suitable to causes material damages.

If the offence is perpetrated against the character of the State including the President of the Republic, Parliament, Constitutional Court, Government bodies and other Constitutional bodies, the sanction is increased by half.

If the offence causes danger for public safety or national economy, the prison sentence ranges from five to ten years.

Mitigating circumstances, other than ones under art. 98 and 114, along with aggravating circumstances under third and fourth paragraphs, may not be considered equivalent or prevailing and any reduction may apply only where aggravating circumstances applied".

- **Terrorist attack with nuclear weapons (art. 280-ter of C.P.)**

"Prison sentence not lower than fifteen years shall apply to anyone who for terrorism purposes as per art. 270-sexies:

1) provides for himself or to other any radioactive material;

2) manufactures or receives a nuclear weapon.

Prison sentence not lower than twenty-five years shall apply to anyone who for terrorism purposes as per art. 270-sexies:

1) uses radioactive material or nuclear weapon;

2) tamper or damages a nuclear plan such that radioactive material may be released.

Sanctions of first and second paragraphs apply also to chemical or bacteriological materials".

The offence is perpetrated under par. 1, 1) applies when a subject provides for himself or to other any radioactive material regardless how it was provided and any related payment. The offence under par. 1, 2) applies when a subject manufactures or assembles a nuclear weapon or receives it.

The offences is perpetrated under par. 2 are more serious than par. 1 and relate to usage of material or weapon (no. 1) or plant (no. 2) regardless the potential hazard or damages caused.

- **kidnapping for purposes of terrorism or for subversion of the democratic order (art. 289-bis of C.P.)**

"Anyone who, for purposes of terrorism or subversion, kidnaps a person is punished with a prison sentence from twenty-five to thirty years.

If the kidnapping results in the death of the kidnapped person and this is an unwanted consequence of the offender's part, the offender shall be punished by imprisonment for thirty years.

If the offender causes the death of the kidnapped person, imprisonment for life shall be imposed.

An accomplice, who, by withdrawing from the association, seeks to allow the victim to regain his/her freedom, is punished with a prison sentence from two to eight years; nevertheless, if the victim, once released, deceases as a consequence of the kidnapping, the prison sentence may range from eight to eighteen years.

Whenever a mitigating circumstance applies, imprisonment for between twenty and twenty-four years shall be substituted for the punishment as per the second paragraph; imprisonment for between twenty-four and thirty years shall be substituted for the punishment as per the third paragraph. Where more than one mitigating circumstances apply, the punishment to be imposed as resulting from the application of the above reductions shall not be less than ten years in the case as per the second paragraph and not less than fifteen years in the case as per the third paragraph".

The offence relates to kidnapping for purposes of terrorism or for subversion of the democratic order. A more serious offence applies when kidnapping results in the death, voluntary or unvoluntary, of the kidnapped person.

- **Incitement to perpetrate crimes against the character of the State c (art. 302 of C.P.)**

"Whosoever incites any person to commit one of the intentional crimes provided for in Book II, Chapters I and II, Title I, shall be punished, if the incitement is unsuccessful, or if the incitement is successful but the crime is not committed, by a prison sentence of one to eight years. Sanction shall be increased up to two thirds in the offence is perpetrated via electronic or telecommunication devices.

However, the sentence shall not be more than one-half the sentence prescribed for the crime that was incited".

The offence is perpetrated by anyone who incites to commit one of the intentional crimes against the character of the State, which are punished with life or prison sentence. Mitigating circumstances apply if incitement is rejected or, if accepted the offence is not perpetrated.

- **Conspiracies to perpetrate crimes against the character of the State by means of an agreement (art. 304 of C.P.)**

"When any person agrees with others for the purpose of committing one of the crimes described in art. 302, participants are punished, if the offence is not perpetrated, with a prison sentence from one to six years.

Sanction is increased for those subjects promoting the agreement.

However, the sentence shall not be more than one-half the sentence prescribed for the crime that was incited".

The offence is perpetrated simply by participating to the association or agreement between at least two persons and aimed at perpetrating one or more crimes under art. 302: it is therefore an offence mainly with by a psychological content where the willingness is punished. The agreement shall exists regardless the availability of means, its format (implicit or explicit) and any conditions; it may not apply if participants are physically or morally forced or unable to understand.

- **Conspiracies to perpetrate crimes against the character of the State by means of association (art. 305 of C.P.)**

"When three or more person associate for the purpose of committing one of the crimes described in art. 302, subjects who promote, set up or organise the association are punished, for this sole purpose, with a prison sentence from five to twelve years.

Participants to the association are punished with a prison sentence from two to eight years.

Leaders of the associations are subject to the same sanctions of the promoters.

The sanctions are increased if the association perpetrates two or more of the aforementioned offences".

The offence is perpetrated when the association between three or more persons is established with the aim to commit one or more offences under art. 302. Those joining the association at a later stage are deemed liable for the crime at the time of joining.

- **Armed conspiracy: establishment and participation (art. 306 of C.P.)**

"When an armed conspiracy is established, with the aim to commit one of the offences under art. 302, those subjects who promote, set up or organise the band are punished, for this sole purpose, with a prison sentence from five to fifteen years.

Participants to the armed conspiracy are punished with a prison sentence from three to nine years.

Leaders of the conspiracy are subject to the same sanctions of the promoters".

The offence is perpetrated when the armed conspiracy is established with the aim to commit one or more offences under art. 302.

- **Assistance to participants of the armed conspiracy (art. 307 of C.P.)**

"Anyone who, with the exception of participation in the crime or of complicity, offers refuge, board, hospitality, means of transportation or communication devices to any person participating in the association or the conspiracy mentioned in previous articles, is punished with a prison sentence up to two years.

The sanction is increased if assistance is provided continuously

Those who commit the fact in favour of a close relative are not subject to punishment.

The incriminated conduct includes offering refuge, board, hospitality, means of transportation or communication devices to any person participating in the association or the conspiracy mentioned in previous articles. It is required the willingness and freedom to provide assistance to participants the association or conspiracy under any type of physical or moral constriction.

- **Gaining possession, Hijacking and destruction of airplane (art. 1 of Law no. 342/1976)**

" Anyone who, with violence or threat, gains possession, hijacks or destroys an airplane is punished with a prison sentence from seven to twenty-one years.

The sanction is increased if the offender is successful in achieving his/her purpose.

Prison sentence may not be lower than twelve years if the offence caused personal injuries to passengers or members of the crew.

Prison sentence may range from twenty-four to thirty years if the offence caused death of one or more persons".

The incriminated conduct refers to gain possession of an airplane with the aim to hijack or destroy it by means of violence, threat or fraud.

- **Damaging landing systems (art. 2 of Law no. 342/1976)**

"Anyone who, with the aim to hijack or destroy an airplane, damages or alters landing systems is punished with sanctions included in the previous articles".

The incriminated conduct refers to the damages caused to the landing systems with the aim to hijack or destroy an airplane.

- **Sanctions (art. 3 of Law no. 422/1989)**

"Anyone who, with violence or threat, gains possession or controls a ship or fixed premises is punished with a prison sentence from eight to twenty-four years.

Same sanction applies to anyone who endangers navigation or safety of fixed premises by:

a) destroying or damaging the ship, freight or fixed premises;

b) destroying, damaging seriously or altering ship navigation systems;

c) communicating intentionally false information on navigation;

d) using violence against person of the ship or fixed premises.

Anyone who threatens to commit one of the crimes of letters a), b), d) of par. 2 is punished with prison sentence from one to three years.

Anyone who, by perpetrating offences under par. 1 and 2, causes the death of a person is punished with life sentence.

Anyone who, by perpetrating offences under par. 1 and 2, causes personal injuries is punished according to art. 582 and 583 of the criminal law with augmented sanctions.

When the action, damages or hazard is of minor entity, sanctions of par. 1 and 2 are reduced from one to two third.

Provisions of current articles do not apply if a major crime is perpetrated".

- **Active repentance (art. 5 of D.Lgs. no. 625/1979)**

"Excluding circumstances mentioned in the last paragraph of art. 56 of the criminal law, it is not punishable the culprit for an offence committed for purposes of terrorism or subversion of the democratic order, who voluntarily prevents the event and gives decisive evidence for the precise reconstruction of the fact and the location of possible accomplices".

- **New York convention - 9 December 1999 (art. 2)**

"*1. Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:*

(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or

(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

2. (a) On depositing its instrument of ratification, acceptance, approval or accession, a State Party which is not a party to a treaty listed in the annex may declare that, in the application of this Convention to the State Party, the treaty shall be deemed not to be included in the annex referred to in paragraph 1, subparagraph (a). The declaration shall cease to have effect as soon as the treaty enters into force for the State Party, which shall notify the depositary of this fact;

(b) When a State Party ceases to be a party to a treaty listed in the annex, it may make a declaration as provided for in this article, with respect to that treaty.

3. For an act to constitute an offence set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offence referred to in paragraph 1, subparagraphs (a) or (b).

4. Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1 of this article.

5. Any person also commits an offence if that person:

(a) Participates as an accomplice in an offence as set forth in paragraph 1 or 4 of this article;

(b) Organizes or directs others to commit an offence as set forth in paragraph 1 or 4 of this article;

(c) Contributes to the commission of one or more offences as set forth in paragraphs 1 or 4 of this article by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) Be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of an offence as set forth in paragraph 1 of this article; or (ii) Be made in the knowledge of the intention of the group to commit an offence as set forth in paragraph 1 of this article".

According to the analysis conducted, art. 2 of New York convention may apply to the Company in relation to actions taken by any means, directly or indirectly, unlawfully and wilfully, to provide or collect funds with the intention that they should be used for terrorism including: airplanes hijacking, attack of diplomatic agents, kidnapping, unlawful manufacturing of nuclear weapons, ship hijacking, etc.

In these circumstances the individual or the entity financing or cooperating shall be aware of the criminal intentions.

It is furthermore applicable the crime under art. 270-quinquies. 1 of C.P." Financing terrorist activities".

3. Areas and Divisions exposed to risk of unlawful conducts

Given the sensitive activities identified during the mapping process, the following list identifies those Areas and Divisions and relevant subjects involved in the sensitive activities:

- Chief Executive Officer;
- Business;
- Legal;
- Occupational safety and health;
- IT;
- Administration, Finance and Audit;
- Marketing;
- Compliance;
- Procurement of goods and services;
- HR.

4. Sensitive activities related to crimes for purpose of terrorism or subversion

After performing controls and risk self-assessment activities (part of the Model), the Company identified the following sensitive activities potentially leading to crimes set forth by art. 25-quarter of the Decree:

- ✓ Management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement;

- ✓ Management of relations with final customers, including set up of minimum requirements, due diligence, qualifications, screening and management of contractual agreement and finalisation of the gambling account;

- ✓ Acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events);

- ✓ Treasury activities including cash movements of bank accounts;

- ✓ Management of residual betting and relations with bookmakers at the end of the horseracing event, including storage of *borderau* and update of MIPAAF account;

- ✓ Ordinary and extraordinary maintenance of horseracing tracks (including premises, equipment, races, green areas, etc.);

- ✓ Management of real estate assets rented to horserace operators (e.g. restaurant, clinic, golf, etc.);
- ✓ Management of horseracing events and other events (concerts, markets, etc.): selection of counterparty, assessment, management of contractual agreement and support of supplier.

Any further addition to the above Sensitive Activities may be proposed to the Board of Directors by the SB and other supervisory entities within the Company. These additions may occur following any change or evolution of the business and activities conducted by each Divisions/Units.

5. Specific prevention protocols

For transactions related to: **management of relations with business partners (Gaming machines, financial institutions, etc.) including the set up of minimum requirements, qualifications, screening and management of contractual agreement**. The provisions of par. 5 of Special Section B - Corporate offences – apply in relation to the sensitive activities in addition to the following:

- ✓ Assess any eventual inclusion of the counterparty in international and national anti-terrorism list (available on the website http://www.bancaditalia.it/UIF/terrorismo/liste);
- ✓ Preliminary check whether counterparty is resident in one of the Countries included in the NCCT list available on the website FATF – GAFI (www.fatf-gafi.org);
- ✓ Any commercial relation with counterparties suspected to be linked to terrorism shall be preliminary authorised by the Board of Directors and reported to the SB;
- ✓ If the counterparty is included in one of the list mentioned above it is strictly forbidden to deal;
- ✓ Before dealing with counterparties, the Company shall assess reputation and reliability of the counterparty, which must be informed of key principles of the Ethical Code and Model.

For transactions related to: **management of relations with final customers, including set up of minimum requirements, due diligence, qualifications, screening and management of contractual agreement and finalisation of the gambling account; acceptance, accounting and payment of any winning and management of related monetary flows (e.g. VLT and Betting above threshold or particular events); management of residual betting and relations with bookmakers at the end of the horseracing event, including storage of *borderau* and update of MIPAAF account; management of real estate assets rented to horserace operators (e.g. restaurant, clinic, golf, etc.); management of horseracing events and other events (concerts, markets, etc.): selection of counterparty, assessment, management of contractual agreement and support of supplier**. The provisions of par. 5 of Special Section E – Offences related to handling stolen goods, laundering and self-laundering, use of money, assets or benefits of illegal origin – apply in relation to the sensitive activities.

For transactions related to: **treasury activities including cash movements of bank accounts**. The provisions of par. 5 of Special Section B - Corporate offences – apply in relation to the sensitive activities in addition to the following:

- ✓ Set up specific limits on transaction type, frequency and amount applicable to any person in charge of using financial resources; furthermore joint signature shall be introduced above certain threshold;

- ✓ To manage cash inflows and outflow, the Company shall rely exclusively on financial channels of EU-based financial institutions and intermediaries or non EU-based institutions subject in any case to similar provisions on money laundering;

- ✓ Limit the use of cash to minor value expenses, which must be duly authorised by competent functions;

- ✓ Transactions involving economical or financial resources shall report explicit reason for payment and must be documented and stored in accordance with fairness and accounting transparency principles;

- ✓ Money collection and payment are always traceable and documented;

- ✓ Prohibition to make/accept payments from subjects holding bank accounts in countries included in "Black List" or "Grey List" unless they live or work in these countries;

- ▪ Prohibition to make/accept payments from counterparties included in international and national anti-terrorism lists (available on the website http://www.bancaditalia.it/UIF/terrorismo/liste) unless there is a written authorisation by the Chief Executive Officer;

- ✓ Prohibition to make/accept payments from counterparties resident in one of the Countries included in the NCCT list available on the website FATF – GAFI (www.fatf-gafi.org);

- ✓ Set up procedures for the CEO to inform and communicate with the SB of any payment made/received by counterparties included in the relevant lists.

6. Information flows to the SB

Persons in charge of relevant functions, who are directly involved in the sensitive activities, shall report periodically any information to the SB in accordance with protocols and procedure "Management of the information flows to the SB".

Furthermore, persons in charge of relevant functions shall promptly inform the SB of any conduct and event diverging from the prevention protocols, even if no offence is perpetrated

7. Disciplinary sanctions

All the provisions included on par. 4 of the General Section of the Model apply in relation to disciplinary sanctions.

Disciplinary system shall apply in the event of any breach of principles, procedures, prevention systems and specific procedures of the current Special Section.