[*Translation from Italian*]

Organization, Management and Control Model Under Leg. Dec. 231/01

of

Conbipel

REVISION	APPROVAL	DESCRIPTION OF CHANGES
Rev. 1	BoD resolution of 19/11/2010	Adoption
Rev. 2	BoD resolution of 09/06/2015	1st Update: ➢ Model adapted to new organization structure ➢ Revision and introduction of environmental offenses, private-to-private corruption
Rev. 3	BoD resolution of 11/05/ 2016	2nd Update: ➢ Revision and introduction of self-laundering ➢ Revision for amendments to the offense of false corporate reporting
Rev. 4	BoD resolution of 11/12/2018	3rd Update: ➢ Model adapted to new organization structure ➢ Revision of the list of offenses after the introduction of: • Illegal intermediation and exploitation of labor • Incitement to private-to-private corruption • Causing illegal entry and abetting of illegal stay (immigration) • Racism and xenophobia ➢ Introduction of a new special section on offenses connected to immigration ➢ Adoption and implementation of the whistleblowing policy

TABLE OF CONTENTS

1. DEFINITIONS 7

2. LEGISLATIVE DECREE NO. 231/2001 AND RELEVANT REGULATIONS 9

3. GUIDELINES OF REFERENCE 14

4. MODEL AND CODE OF ETHICS 16

5. THE MODEL 17

5.1 The Method to Build the Model 17
5.2 The Function of the Model 18
5.3 Principles and Elements Inspiring the Model 18
5.4 The Structure of the Model 20
5.4.1 The Organization and Authorization System 22
5.4.2 Control Principles 22
5.4.3 The Cash Flow Management System 23
5.4.4 General Prevention Principles and Policies 24
5.5 Revising and Adapting the Model 27

6. ORGANIZATION, ADMINISTRATION AND ACCOUNTING ISSUES OF ACTIVITIES AND OPERATIONS . 28

6.1 Introduction 28
6.2 Organization Structure 28
6.2.1 The Organization Structure for Occupational Health and Safety 29
6.2.2 The Organization Structure in the Area of Environment 29
6.3 Manual and Automated Procedures 30

7. SENSITIVE PROCESSES 33

8. THE SURVEILLANCE COMMITTEE (SC) 34

8.1 Identifying the Surveillance Committee 34
8.2 Establishment, Appointment and Replacement of the SC 34
8.3 Financial Resources Allocated to the Surveillance Committee 35
8.4 Functions and Powers of the Surveillance Committee 35
8.5 Reporting of the SC to the Company Top management 37
8.6 Information Flows 38
8.6.1 Whistleblowing 39

9. TRAINING RESOURCES AND DISSEMINATING THE MODEL 42

9.1 Knowledge by and Training to Employees and Company Bodies 42
9.2 Disclosure to Consultants and Partners 43

10. DISCIPLINARY SYSTEM 44

10.1 Function of the Disciplinary System 44
10.2 Structure, Development and Adoption of the Disciplinary System 44
10.3 Measures against Employees 47
10.4 Measures against Executives 49
10.5 Measures against Directors 50
10.6 Measures against Statutory Auditors 50
10.7 Measures against the Members of the SC 50

10.8 Measures against Service Companies, Consultants, Partners....50
10.9 Measures Applicable under Whistleblowing Regulations....50

SPECIAL SECTIONS 52

SPECIAL SECTION A 53

11. OFFENSES IN RELATIONS WITH GOVERNMENT AGENCIES 54

11.1 Cases of Offenses in Relations with Government Agencies (art. 24 and art. 25 of Leg. Dec. 231/2001). 54
11.2 Sensitive Processes in Relations with Government Agencies 54
11.3 The System in General.... 55
11.4 The System of the Delegation of Powers and Powers of Attorney 56
11.5 General Principles of Conduct.... 57
11.6 Specific Procedural Principles.... 59
11.7 Special Procedural Principles in the event of Specific Risk-Featuring Transactions 63

SPECIAL SECTION B 64

12. CORPORATE CRIME 65

12.1 Cases of Corporate Crime (art. 25 ter of Dec. Leg. /2001) 65
12.2 Sensitive Processes in connection with Corporate Crime 65
12.3 General Principles of Conduct.... 67
12.4 Specific Procedural Principles.... 71

SPECIAL SECTION C AND SPECIAL SECTION C-BIS 75

13. RECEIVING, LAUNDERING AND USING CASH, ASSETS OR BENEFITS OF A CRIMINAL ORIGIN, AND SELF-LAUNDERING, AND CRIMES FOR THE PURPOSES OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER 76

13.1 SPECIAL SECTION C: Receiving, Laundering and using Cash, Assets and Benefits of Unlawful Origin (art. 25 octies of Leg. Dec. 231/2001) and Crimes with the purpose of Terrorism or Subversion of the Democratic Order (art. 25 quater Leg. Dec. 231/2001) 76
13.1.1 ... Sensitive Processes in connection with Receiving, Laundering and Using Illegal Benefits and with Crimes with the purpose of Terrorism or Subversion of the Democratic Order 76
13.1.2 ... General Principles of Conduct 78
13.1.3 ... Specific Procedural Principles 79
13.2 SPECIAL SECTION C-BIS: Self-Laundering (art. 25 octies of Leg. Dec. 231/2001)80
13.2.1 ... General Principles of Conduct and Specific Procedural Principles 82

SPECIAL SECTION D 84

14. MANSLAUGHTER AND SERIOUS AND VERY SERIOUS UNINTENTIONAL INJURIES COMMITTED WITH BREACHES OF ACCIDENT-PREVENTION PROVISIONS AND OCCUPATIONAL HEALTH, SAFETY AND HYGIENE LEGISLATION (ART. 25 SEPTIES OF LEG. DEC. 231/2001) 85

14.1 Sensitive processes related to Manslaughter and unintentional serious or very serious injuries committed with breaches of accident-prevention provisions and regulations on the protection of occupational hygiene and health 85
14.2 General Overview 87
14.3 Organization.... 88
14.3.1 ... Identification of the Employer 88

14.3.2 ... Identification of Executives and Supervisors and, in general, Assignment of Duties and Roles 88
14.3.3 ... Designating the Manager of the Internal or External Prevention and Prevention Service, pursuant to art. 32 Leg. Dec. 81/08 88
14.3.4 ... Appointment of the Company Physician in the cases set out in art. 41 Leg. Dec. 81/08 89
14.4 Monitoring – Periodic Audits – Surveillance 90
14.5 Legal Obligations 91
14.6 Investment Plan and Annual Budged for Actions in the area of Occupational Health and Safety and Relevant Reporting 92
14.7 Risk Assessment – Prevention and Protection Measures 93
14.7.1 ... Preparing and Revising the Risk Assessment and the Risk Assessment Document (DVR) under arts. 28 and 29 of Leg. Dec. 81/08 93
14.8 Equipment, Systems, Workplaces; Chemical, Physical and Biological Agents 95
14.9 Organization Operations 96
14.9.1 ... Designation of Workers in charge of Implementing Fire-Prevention and Fire-Fighting measures and of Workers Evacuation in the event of Serious and Immediate Danger, Rescue, First Aid and, in any case, of Emergency Management and Drafting Intervention Measures 96
14.9.2 ... Execution of Agency Work Agreements, Contracts for Works and Subcontracts 97
14.9.3 ... Keeping the Logbook of Injuries and Recording "Near–Misses" (or Accidents with No Injury) .. 97
14.9.4 ... Control of Access to Premises 98
14.10 Health Surveillance 99
14.11 Information and Training 99
14.12 Safe Work Procedures and Instructions 99
14.13 Required Documents and Certificates 99
14.14 Specific Procedural Principles 99
14.14.1 . Individual Protection Devices (DPI) 100
14.15 Traceability 101

SPECIAL SECTION E 102

15. OFFENSES IN THE FIELD OF INDUSTRIAL PROPERTY AND COPYRIGHT / OFFENSES OF DISRUPTION OF COMPETITION 103

15.1 Cases of offenses in the field of Industrial Property and Copyright or Disruption of Competition 103
15.2 Connection of the Special Section "Cybercrime and Illegal Data Processing" with the Offenses in Art. 25-novies of Leg. Dec. 231/01: of Copyright 103
15.3 Sensitive Processes in connection with Offenses in the area of Industrial Property and Copyright and Disruption of Competition 103
15.4 General Principles of Conduct 105
15.5 Specific Procedural Principles 105
15.6 Traceability 106

SPECIAL SECTION F 107

16. COUNTERFEIT MONEY AND COUNTERFEIT DISTINCTIVE SIGNS 108

16.1 Cases of Counterfeit Money, Securities, Official Stamps and Distinctive Signs or Marks (Art. 25 bis Leg. Dec. 231/2001). 108
16.2 Sensitive Processes in the area of Counterfeit Money, Securities, Official Stamps and Distinctive Signs or Marks 108
16.3 General Principles of Conduct 108

16.4 Specific Procedural Principles....109

SPECIAL SECTION G....110

17. CYBERCRIME AND ILLEGAL DATA PROCESSING....111

17.1 Cases of Cybercrime and Illegal Data Processing....111
17.2 Sensitive Processes in the Area of Cybercrime and Illegal Data Processing....111
17.2.1 ... Risk-Featuring Areas 111
17.2.2 ... Sensitive Activities 111
17.3 General Principles of Conduct....112
17.3.1 ... General Principles 112
17.3.2 ... General Principles of Conduct 113
17.4 Specific Procedural Principles....118

SPECIAL SECTION H....120

18. ORGANIZED CRIME....121

18.1 Cases of Organized Crime....121
18.2 Sensitive Processes in connection with Organized Crime....121
18.3 General Principles of Conduct and Specific Prevention Policies....122

SPECIAL SECTION I....124

19. INCITEMENT TO REFRAIN FROM MAKING STATEMENTS OR TO MAKE FALSE STATEMENTS TO THE JUDICIAL AUTHORITY....125

19.1 Cases of Incitement to Refrain From Making Statements or to Make False Statements to the Judicial Authority....125
19.2 Prevention....125
19.3 Specific Procedural Principles....125

SPECIAL SECTION L....126

20. ENVIRONMENTAL CRIME....127

20.1 Cases of Environmental Crimes....127
20.2 Function and Addressees....127
20.3 General Issues....128
20.4 Sensitive Processes in the Area of Environmental Crime....129
20.5 General Principles of Conduct....131
20.6 Specific Procedural Principles....132
20.6.1 ... Management of Statutory Requirements on Liquid Waste 132
20.6.2 ... Implementation of Statutory Requirements on Waste Management 132
20.6.3 ... Implementation of Statutory requirements on Air Emission Management 133
20.6.4 ... Implementation of Statutory Requirements on Ozone-Depleting Substance Management 133
20.6.5 ... The Killing, Destruction, Catching, Possession or Taking of Specimens of Protected Wild Fauna or Flora Species in connection 134
20.6.6 ... Environmental Emergency Management 134
20.6.7 ... Formalization of roles and remit, and related management responsibilities 134
20.6.8 ... Appropriate Information and Training of Workers 134
20.6.9 ... Supervision on Compliance with Environmental Procedures and Instructions 134
20.6.10 . Obtaining Authorizations and Certifications Required by the Law 135
20.6.11 . Periodic Internal Checks on the Application and Effectiveness of Adopted Procedures 135

20.6.12 . Appropriate Control Systems on Maintaining in time Appropriate Conditions of Adopted Environmental Measures and Record Keeping of Completion of the Activities Listed Above 135

20.7 Traceability 135

SPECIAL SECTION M 137

21. TRANSNATIONAL CRIME 138

21.1 Cases of Transnational Crime (Art. 10 Law no. 146 dated 16.3.2006) 138
21.2 Sensitive Processes in the Area of Transnational Crime 138
21.3 General Conduct Principles 138
21.4 Specific Procedural Principles 139

SPECIAL SECTION N 140

22. OFFENSES RELATED TO IMMIGRATION 141

22.1 Cases of Offenses related to Immigration 141
22.2 Sensitive Processes in the area of Offenses related to Immigration 141
22.3 General Principles of Conduct 141

22.3.1 ... General Principles 141

22.3.2 ... General Principles of Conduct and Specific Prevention Policies 142

1. DEFINITIONS

- "Regulatory Authority": judicial authorities, national and foreign government administrations and institutions, Italian competition authority, Italian data protection authority and other Italian and foreign regulatory authorities;
- "CONBIPEL" or the "Company": CONBIPEL S.p.A.;
- "CCNL": National collective bargaining agreement currently in force and applied by CONBIPEL S.p.A.;
- "Code of Conduct" and/or "Code of Ethics": code of ethics adopted by CONBIPEL S.p.A.;
- "Consultants": persons acting in the name and/or on behalf of CONBIPEL S.p.A., based on an engagement or other consultancy contracts;
- "Leg. Dec. 231/2001" or "Decree": legislative decree no. 231 dated 8 June 2001 as subsequently amended;
- "Addressees": Employees, Consultants, Partners, Service Companies, Corporate Bodies and any other person howsoever working for CONBIPEL S.p.A.;
- "Top Managers": persons with representation, administration or management functions of the Company or of one of its financially and functionally independent units, and persons that exercise, including *de facto*, the management and the control on the Company;
- "Subordinates": persons under the direction or supervision of one of the Top Managers and consequently, in practice, all parties that have a subordinate employment relation with the Company;
- "Employee" or "Employees": all employees of CONBIPEL S.p.A.; (including executives);
- "Officer in Charge of Public Services": any person rendering public services that does not have the powers of a public official, or any person that, albeit operating in a field regulated as state function, does not exercise the typical powers of a state function and does not merely carry out clerical tasks nor merely material labor;
- "Guidelines": the Guidelines for drafting organization, management and control models under Leg. Dec. 231/2001 approved by Confindustria on 7 March 2002, as subsequently revised;
- "Models" or "Model": the organization, management and control model or models under Leg. Dec. 231/2001 or this organization, management and control model

prepared to prevent the offenses set out in articles 6 and 7 of the Decree, to supplement organization and control tools already implemented within the Company (Code of Ethics, Operating instructions, Service orders, organizational charts, powers of attorneys, proxies, operating manuals, offense risk maps);

- "Sensitive Operation": an operation or transaction that falls within the scope of Sensitive Processes; it may have a business or financial nature or it may be related to political or corporate lobbying (including, in this latter case: reductions of capital, mergers, demergers, transactions on the shares of the parent company, contributions, reimbursements to shareholders, etc.);

- "Corporate Bodies": the Board of Directors and the Board of Statutory Auditors of CONBIPEL S.p.A.;

- "Surveillance Committee" or "SC": internal committee in charge of surveilling on operation of and compliance with the Model and its revision;

- "G.A." or "GA": Italian and/or foreign Government Agencies, including relevant officials and officers in charge of public services;

- "Partners": contractual parties of CONBIPEL S.p.A., including but not limited to suppliers, agents, trading partners, occasional and permanent resellers, whether individuals or legal entities, with which the Company implements any form of contractually regulated relation (purchase and sale of goods and services, temporary business combines, joint ventures, consortiums, etc.), whose purpose is to cooperate with the Company in connection with Sensitive Processes;

- "Sensitive Processes" or "sensitive processes": CONBIPEL S.p.A.'s operations capable of generating the risk of perpetration of Offenses;

- "Offense" or "Offenses": one or several offenses governed by the provisions of Leg. Dec. 231/2001, as subsequently amended and supplemented;

- "General Rules and Principles": general rules and principles in this Model;

- "Service Company": third party companies that render services to the benefit of CONBIPEL S.p.A..

2. LEGISLATIVE DECREE NO. 231/2001 AND RELEVANT REGULATIONS

On 8 June 2001, implementing the delegation in article 11 of Law no. 300 of 29 September 2000, Legislative Decree 231/2001 was introduced and it became effective on 4 July 2001. The aim of Leg. Dec. 231/2001 was to adapt domestic legislation on the liability of legal entities to certain international conventions that Italy had signed[1] in the past.

Leg. Dec. 231/2001 on "*Rules on the administrative liability of legal persons, companies and associations including with no legal personality*", introduced for the first time in Italy liability in a criminal court[2] of entities for certain offenses committed in their interest or to their benefit by persons that have representation, administration or management functions within the entity or of one of its financially and functionally independent units, as well as persons that exercise, including *de facto,* its management and control and, finally, persons under the management or supervision of one of the persons indicated above.

This liability is in addition to the responsibility of the individual who materially perpetrated the offense.

This new liability introduced by Leg. Dec. 231/2001 aims at involving in the punishment of certain criminal offenses the assets of the entities that took advantage of the perpetrated crime.

The key elements of the Decree concern:

a) the type of crime contemplated to date;

b) penalties;

c) parties involved;

[1] Delegation law no. 300, of 29 September 2000, ratified and followed several international instruments, developed based on the Treaty on European Union, including:

- Convention of the European Community on the protection of financial interests (Brussels, 26 July 1995);
- Convention on the fight against corruption involving officials of the European Communities or of Member States (Brussels of 26 May 1997);
- OECD Convention Combating Bribery of Foreign Public Officials in International Business Transactions (Paris, 17 December 1997).

[2] The nature of this new kind of liability introduced in the Italian legal framework by Leg. Dec. 231/2001 was the topic of an extensive debate: the punishing nature of penalties that may be inflicted on the entity, the fact that such liability is triggered by perpetration of a crime and is determined through a criminal trial against the person who materially committed it, support the opinion of those who uphold that this is a "semi-criminal" liability that is "of a third category that embodies the essential elements of the criminal system and of the administrative law system in an attempt to balance the reasons of effective prevention with the reasons – that are even more unavoidable – of the utmost guarantee " (Explanatory Report).
Court of Cassation, no. 3615, 20 December 2005 "Despite the legal name, the new liability, nominally administrative, conceals its essentially criminal nature; this may have been understated to avoid opening critical conflicts with the principles that criminal indictment is strictly personal, as stated in the Constitution (art. 27 Cost.); these may be construed reductively as no liability for an event committed by another person or more broadly as no liability for events that are out of one's control."

d) organization and management models.

The legislation under review currently applies to the following ten types of **offenses**:

a) Offenses committed in relations with Government Agencies (art. 24 and art. 25 Leg. Dec. 231/2001),

b) Cybercrime and illegal data processing (art. 24 bis Leg. Dec. 231/2001),

c) Organized crime (art. 24 ter Leg. Dec. 231/2001),

d) Counterfeit money, securities, official stamps and distinctive signs (art. 25 bis Leg. Dec. 231/2001),

e) Offenses against industry and trade (art. 25 bis1 Leg. Dec. 231/2001),

f) Certain offenses in the area of corporate crimes and the offense of private-to-private corruption (art. 25 ter Leg. Dec. 231/2001),

g) Crimes for the purposes of terrorism or subversion of the democratic order (art. 25 quater Leg. Dec. 231/2001),

h) Offenses connected to "crimes" against individuals (arts. 25 quater1 and quinquies Leg. Dec. 231/2001),

i) Market abuse (art. 25 sexies Leg. Dec. 231/2001),

j) Manslaughter and serious or very serious injuries committed with breaches of accident-prevention provisions and/or occupational health and safety legislation (art. 25 septies Leg. Dec. 231/2001),

k) Receiving, laundering and using cash, assets or benefits of a criminal origin, and self-laundering (art. 25 octies Leg. Dec. 231/2001),

l) Offenses in the field of copyright infringement (art. 25 novies Leg. Dec. 231/2001),

m) Offense of incitement to refrain from making statements or to make false statements to the judicial authority (art. 25 decies Leg. Dec. 231/2001),

n) Environmental crimes (art. 25 undecies Leg. Dec. 231/2001),

o) Transnational crime[3],

p) Employment of illegally staying third-country nationals (art. 25-duodecies Leg. Dec. 231/2001),

q) Racism and xenophobia (art. 25-terdecies Leg. Dec. 231/2001)[4].

[3] This type of crime was introduced by Law no. 146 dated 16 March 2006.

[4] The list of offenses has been expanded since its original introduction in the Decree. The following legislation added offenses: Law Decree no. 350 of 25 September 2001, which introduced art. 25-bis «Counterfeit money, securities and official tax stamps», then expanded and amended into «Offenses of counterfeit money, securities, tax stamps and distinctive signs» by Law no. 99 of 23 July 2009; Legislative Decree no. 61 dated 11 April 2002, which introduced art. 25-ter «Corporate crime »; Law no. 7 of 14 January 2003, which introduced art. 25-quater

A **fine** always applies to all offenses and it is calculated in units (between one hundred and one thousand units, without prejudice to the mitigating and aggravating circumstances, as specifically determined in Leg. Dec. 231/2001), each of which ranges from a minimum of Euro 258 to a maximum of Euro 1549 (identified, in practice, based on the economic and financial position of the entity and the effectiveness of the fine).

Certain predicate offenses also trigger **prohibition measures** such as disqualification from the business, suspension or revocation of authorizations, licenses or permits that are functional to the perpetration of the offense, prohibition to enter into agreements with GA, exclusion from contributions, loans, grants or subsidies, and the possible revocation of any contributions, loans, grants, or subsidies that were already granted, prohibition to advertise goods and services.

An addition mandatory major penalty is **confiscation** of the price or profit of the offense. This is always ordered against the entity in the guilty verdict, except for such part of the price or profit that may be given back to the damaged party and without prejudice to any rights acquired by third parties in good faith.

Confiscation may be enforced as "value-based confiscation", meaning by removing amounts of cash, assets or other benefits whose value matches the price or profit of the offense.

Finally, in the event of application of penalties that are prohibitions, the judge may order publication of the guilty verdict against the entity, which shall also bear the costs for such publication.

In case of **disqualification**, if there is serious indicative evidence of the entity's liability and there are founded and specific elements of reiteration of perpetration of the offense, **precautionary measures** may be applied.

«Crimes with the purpose of terrorism or subversion of the democratic order»; Law no. 228 of 11 August 2003, which introduced art. 25-quinquies «Crimes against individuals »; Law no. 62 of 18 April 2005, which introduced art. 25-sexies «Market abuse»; Law no. 7 of 9 January 2006, which introduced art. 25-quater.1 «Female genital mutilation practices»; Law no. 146 of 16 March 2006, which sets out liability of entities for transnational crimes; Law no. 123 of 3 August 2007, which introduced art. 25-septies «Manslaughter and serious or very serious injuries committed with breaches of accident-prevention provisions and/or occupational health and safety legislation», later amended into «Manslaughter and serious or very serious injuries committed with breaches of occupational health and safety regulations» by Legislative Decree no. 81 of 9 April 2008; Legislative Decree no. 231 of 21 November 2007, which introduced art. 25-octies «Receiving, laundering and using cash, assets or benefits of a criminal origin, and self-laundering»; Law no. 48 of 18 March 2008, which introduced art. 24-bis «Cybercrime and illegal data processing»; Law no. 94 of 15 July 2009, which introduced art. 24-ter «Organized crime»; Law no. 99 of 23 July 2009 – referred to above – which introduced art. 25-bis.1 «Offenses against industry and trade » and art. 25-novies «Offenses in the field of copyright infringement»; Law no. 116 of 3 August 2009, which introduced art. 25-novies (later renumbered art. 25-decies by Legislative Decree no. 121 of 7 July 2011, no. 121) «Incitement to refrain from making statements or to make false statements to the judicial authority»; Legislative Decree no. 121/2011 – referred to above – which introduced art. 25-undecies «Environmental crimes»; Legislative Decree no. 109 of 16 July 2012, which introduced art. 25-duodecies «Employment of illegally staying third-country nationals»; art. 5, of Chapter II of Law no. 167 of 20 November 2017 (European Law 2017), which introduced art. 25-terdecies «Racism and xenophobia».

Precautionary measures may consist in **seizure** enforced on all things which may be confiscated.

Prohibition measures apply only in connection with offenses for which they are expressly set out when at least one of the following conditions is met (art. 13, para. 1 of the Decree): (i) from the offense the entity drew a *significant profit* and the offense was committed by *top managers* or by *persons under the supervision of others* when, in the latter case, perpetration of the offense was determined or made easier by serious shortcomings in the organization; (ii) in the event of *reiteration of offenses*.

Disqualification from exercising the business, the prohibition to enter into agreements with Government Agencies and to advertise goods or services may apply permanently, in extremely serious cases (art. 16 of the Decree).

With respect to **involved parties**, under Leg. Dec. 231/2001, the entity is responsible for offenses committed in its interest or to its benefit by:

i. "*persons with representation, administration or management functions within the entity or one of its financially and functionally independent organization units, and by persons that exercise, including* de facto, *management and control of the entity*" (so-called "top managers"; art. 5, para. 1, lett. a) of the Decree);

ii. by persons under the management or supervision of top managers (so-called "persons under the management of others", art. 5, para. 1, lett. b) of the Decree).

The law expressly provides (art. 5, para. 2 of the Decree) that the entity is not accountable if such persons acted only in their interest or in the interest of third parties.

In the event of an offense committed by a top managers, the entity is not accountable if it proves that (art. 6, para. 1 of the Decree):

a) the management body effectively adopted, before perpetration of the event, organization, management and control models fit to prevent the offenses that were committed;

b) the responsibility of monitoring operation and effectiveness of and compliance with the models, and to see to their revision, was entrusted to an internal committee with independent powers of initiative and control;

c) individuals committed offenses by dodging fraudulently organization and management models;

d) there was no omitted or insufficient monitoring by the committee referred to in letter b) above.[5]

[5] The Explanatory Report to the Decree underlines, in this respect: *"the starting point is the (empirically grounded presumption) that, if an offense is perpetrated by top management, the "personal" element of the entity's responsibility* [meaning the so-called "fault in organization " of the entity] *is met, since top management expresses and represent the entity's policy; where this does not happen, the company will have to prove its lack of responsibility and it may do so only by demonstrating that a series of concurrent conditions are met".*

The Decree outlines the contents of **organization and management models** (art. 6, para. 2 of the Decree) and sets out that they must cater for the following needs, based on the extent of the delegated powers and the risk of committing offenses:

a) identify tasks where Offenses may be committed;

b) prepare specific policies aimed at planning the making and implementation of the entity's decisions in connection with Offenses that need to be prevented;

c) identify how to manage financial resources appropriate to prevent perpetration of the Offenses;

d) set out disclosure obligations with the body responsible for monitoring operation of and compliance with the organization model;

e) introduce a disciplinary system appropriate to punish failure to comply with the measures in the organization model.

If an Offense is committed by persons under the management of others (art. 7 of the Decree), the entity is not accountable if it proves that failure to comply with management or supervisory obligations did not contribute to perpetration of the Offense. In any event, the entity is not accountable if, prior to perpetration of the Offense, it had adopted and effectively implemented an organization, management and control model appropriate to prevent the type of offense that was committed.

Organization and management models may be adopted based on code of conducts prepared by associations that represent entities and notified to the Ministry of Justice, which, together with the relevant Ministers, may express comments on the appropriateness of such models to prevent offenses within 30 days (art. 6, para. 3 of the Decree).

CONBIPEL S.p.A. intends to adopt the provisions of the Decree with the goal of preventing perpetration of Offenses, by adopting an Organization, Management and Control Model and by drawing inspiration, in drafting the latter, from the Guidelines prepared by Confindustria.

3. GUIDELINES OF REFERENCE

In adapting its organization and corporate structures to the provisions of Leg. Dec. 231/2001, or in preparing this Model, CONBIPEL S.p.A. was inspired by the Guidelines.

This decision was taken based on and in consideration of Confindustria's latest revision of its Guidelines[6]. To be in a position to provide a useful tool appropriate to evolving legislation, Guidelines are constantly revised. It is understood that the choice to refrain from aligning Model to certain indications in the Guidelines does not affect its validity. Since the Model needs to be adjusted to the specific situation of the Company, it may depart from the Guidelines which have, inherently, a general nature.

The Guidelines identify the essential features to build a Model in the following steps:

1. Identifying risks, i.e. the review of company structure to point out in which areas/segments and how offenses set out in the Decree may be perpetrated;
2. Planning the control system (so-called policies), i.e. assessing the existing control system and any adjustment to effectively contrast any previously identified risks.

Confindustria identifies the following elements for a control system to prevent offenses committed with willful intent, which must be implemented at Company level to ensure an effective Model:

a) Adoption of a code of ethics with reference to offenses under review;

b) Adopting a clear and official organization system, especially with respect to accountability;

c) Adoption of manual and automated procedures;

d) Adoption of a system of authorizations and signature powers;

e) Adoption of a management control system;

f) Adoption of a disclosure and training system for HR.

The above components must be inspired by the following principles:

a) Each transaction, settlement, action must be verifiable, documented, consistent and appropriate;

b) No one may manage an entire process independently;

c) The control system must track and keep record completed checks.

These principles are discussed in detail in the following chapters.

3. Appointing a Surveillance Committee, i.e. the body which is entrusted with the task of monitoring operation of and compliance with the Model and see to its revision;

[6] The Ministry regarded the revision of the Guidelines of reference in force in March 2014 as: "overall appropriate and fit to achieve the goal set in art. 6, para. 3, of Leg. Dec. 231/2001".

4. Defining an independent disciplinary system with punishment mechanisms applicable to breaches of the Code of Ethics and the Model's procedures.

4. MODEL AND CODE OF ETHICS

The rules of conduct in this Model are consistent with the rules of the Code of Ethics, as adopted by the Company, even if the purpose of this Model is specifically to comply with Leg. Dec. 231/2001.

Indeed:

- The Code of Ethics has been adopted independently and it is applied generally by the Company with a view to expressing principles of "corporate ethics", which the Company recognizes as its own and which it requires all Employees, Corporate Bodies, Consultants and Partners to comply with;
- The Model instead reflects specific requirements in Leg. Dec. 231/2001, aimed at preventing perpetration of specific types of offenses (for events that, apparently committed to the benefit of the company, may trigger administrative liability from an offense based on the provisions of the Decree). The Model sets rules and procedures that must be complied with to exempt the Company from liability under Leg. Dec. 231/2001.

5. THE MODEL

5.1 THE METHOD TO BUILD THE MODEL

Adoption of an Organization, management and control Model pursuant to the Decree, along with the simultaneous presence of the Code of Ethics, in addition to being a cause for exemption from liability for the Company with respect to the perpetration of certain types of offenses, is also an act of corporate social responsibility, which generates benefits for all the stakeholders: shareholders, users, employees, creditors and all other parties whose interests are connected to the fate of the Company.

Introducing an additional control system, along with the definition and dissemination of ethical principles that increase already high standards of conduct adopted by the Company on the one hand increases the good reputation and trust that third parties identify with CONBIPEL (an asset of increasing value for companies) and, more importantly, has a regulatory function. These tools, indeed, contribute to regulating conducts and decisions of anyone who is called daily to operate in the name or to the benefit of the Company, pursuant to such ethical principles and standards of conduct.

Thus, CONBIPEL's intention was to start a series of tasks aimed at making its organization model consistent with the Decree's requirement, with the principles already rooted in its governance culture, and with the indications in the Guidelines. To such effect, a process was activated to draft, and subsequently revise and update, the Model (hereinafter the "Project"), based on the evolution of legislation, best practices and the Company's organization and actual situation.

The selected method to implement the Project, in terms of organization, definition of operating methods, definition of steps, attribution of responsibilities to the various corporate functions, was developed to ensure the quality and reliability of the outcome. The Project included the steps that are briefly recapped below:

Step	*Task*
Step 1	***Launching the Project and identifying processes and tasks in whose scope offenses referred to in Leg. Dec. 231/2001 may be committed*** *Collecting and reviewing documents, preliminarily identifying processes/tasks in whose scope the offenses referred to in the Decree may be committed (so-called "sensitive" processes/activities).*
Step 2	***Identifying key officers*** Identifying key officers, meaning the persons within the Company that, based on their functions and responsibilities, have an in-depth knowledge of sensitive areas/activities, and of control mechanisms currently in place, to determine the scope of the action and a detailed interview schedule.
Step 3	***Analyzing sensitive processes and activities*** Identifying and analyzing sensitive processes and activities, and existing control mechanisms, with specific attention to prior review and other compliance elements/tasks.
Step 4	***Identifying control policies*** Identifying organization requirements that characterize an appropriate organization, management and control model pursuant to the Decree and control policies with the function of preventing offenses, in consideration of procedures already existing in CONBIPEL.
Step 5	***Defining the organization, management and control model*** Defining the organization, management and control model pursuant to the Decree, inclusive of all its components and operating rules.

5.2 THE FUNCTION OF THE MODEL

Adoption and effective implementation of the Model not only allow the Company to benefit from the exemption in Leg. Dec. 231/2001 but also improve, within its scope, its Organization Structure, curtailing the risk of committing Offenses.

The purpose of the Model is to set up a structured and organic system of (prior and ex post) procedures and review activities whose goal is to reduce the risk of perpetration of Offenses by identifying Sensitive Processes and setting out procedures applicable to such processes.

The principles in this Model must lead, on the one hand, to causing those who act on behalf Company to refrain from committing illegal conducts (whose perpetration is strongly condemned and contrary to the interests of the Company, even when the latter could apparently draw an advantage from it) including by orienting their operations, on the other, thanks to the constant monitoring of operations, to allow the company to prevent or avert perpetration of Offenses by enabling it to react without delay, including at disciplinary level, in the event of conducts that breach the Model.

The goals of the Model therefore include to develop awareness in Employees, Corporate Bodies, Service Companies, Consultants and Partners operating on behalf or in the interest of the Company in Sensitive Processes that they may incur, in the event of conducts that do not comply with the requirements of the Code of Conduct and other Company rules and procedures (and of the law), in possible consequences that are relevant with respect to criminal law, not only personally but also for the Company.

Moreover, it intends to actively condemn any unlawful conduct through the constant work of the Surveillance Committee on the operations of persons with respect to Sensitive Process and through the application of disciplinary or contractual penalties.

5.3 PRINCIPLES AND ELEMENTS INSPIRING THE MODEL

In preparing this Model, existing procedures and control systems were taken into account "as-is", in that they were already fully operating in the Company, when regarded as appropriate to apply as measures to prevent Offenses and to control Sensitive Processes.

Without prejudice to its specific role in connection with Leg. Dec. 231/2001, this Model is part of a broader control system, mainly comprising the rules of the organization structure and the internal control system.

Namely, the Company identified the following specific tools aimed at taking and implementing the Company's decisions in connection, among other things, with Offenses that need to be prevented:

1) internal control system and, accordingly, all Company regulations (standards, manual and automated procedures, manuals, operating instructions, guidelines,

policies, regulations, etc.) concerning all corporate systems (quality management system, management control and reporting system, administrative, accounting and financial system, industrial and environmental safety management system, etc.), the documents and provisions related to the reporting-functional and organizational structure of the Company, and the organized system of delegated powers and proxies;

2) Code of Ethics, which also includes by reference the principles in item 1) above;
3) Disclosure to staff and their training;
4) disciplinary system in the CCNL;
5) In general, any applicable Italian and foreign legislation.

The principles, rules and procedures in the tools listed above are not stated in detail in this Model, but are part of the organization and control system which it supplements, and they were reviewed when building the Model.

In addition to the foregoing, the key principles of the Model are:

a) Confindustria's Guidelines, based on which Sensitive Processes were mapped;

b) The requirements under Leg. Dec. 231/2001 and specifically:
   - Entrusting a Surveillance Committee (SC) with the task of promoting the effective and correct implementation of the Model including by monitoring corporate conducts and the right to constant information on any operations that are relevant for the purposes of Leg. Dec. 231/2001;
   - Allocating (and making available) to the SC appropriate resources to support it in its tasks and in achieving reasonable results;
   - Audits of operation of the Model and its consequent periodic revision (*ex post* review);
   - Disclosing and making all Addressees of this Model aware of rules of conducts, implemented procedures, guidelines and corporate policies;

c) The general principles of an appropriate internal control system and specifically:
   - The existence of a body of manual and automated policies and procedures capable of regulating and governing all so-called sensitive activities (*Procedures*);
   - The possibility to trace and document all transactions that are relevant under Leg. Dec. 231/2001 (*Monitoring and Traceability*);
   - Compliance with the principle of segregated functions (*Segregation*);
   - The definition of authorization powers that are consistent with assigned responsibilities (*Delegated Powers*);
   - Disclosure to the SC of all relevant information;

d) Finally, in implementing the control system, albeit with the required general audit operations on the business, priority has to be given to areas that feature a

significant chance of Offenses being perpetrated and a high value/relevance of Sensitive Operations.

5.4 THE STRUCTURE OF THE MODEL

In light of the indications described in the previous paragraphs, the Company intended to prepare a Model that, based on its experience and the indications in court decisions concerning this subject, is an appropriate tool to fight against the possible perpetration of offenses, consistently with the governance system and the ethical values which have always inspired the Company.

The Model, as prepared further to the above activities, comprises:

a) a **General Section**, whose function is to define the general principles that the Company sets as reference for the operation of its business and that are valid for the business situation in a broad sense and not only in carrying our activities that feature risks. This section summarizes or includes as annexes the following elements which are a material part of the General Section:

   1) Organization chart;

   2) Code of Ethics;

   3) Surveillance Committee and its operation;

   4) Disciplinary system;

b) Several **Special Sections** that describe, with reference to specific offenses, the mapping of sensitive activities, the assessment / setup / adjustment of prior reviews, and relevant specific policies. Their function is to:

   - determine the sources or regulations which Addressees must abide by;
   - identify conduct principles to implement;
   - identify each offense that may in practice and potentially be committed within the Company and relevant prevention measures.

The Model currently has the following Special Sections:

1. **SPECIAL SECTION A**: OFFENSES IN RELATION WITH GOVERNMENT AGENCIES
2. **SPECIAL SECTION B**: CORPORATE OFFENSES
3. **SPECIAL SECTION C and SPECIAL SECTION C-BIS**: RECEIVING, LAUNDERING AND USING CASH, ASSETS OR BENEFITS OF A CRIMINAL ORIGIN, AND SELF-

LAUNDERING AND CRIMES FOR THE PURPOSE OF TERRORISM AND SUBVERSION OF THE DEMOCRATIC ORDER

4. **SPECIAL SECTION D**: MANSLAUGHTER AND SERIOUS OR VERY SERIOUS INJURIES COMMITTED WITH BREACHES OF ACCIDENT-PREVENTION PROVISIONS AND/OR OCCUPATIONAL HEALTH AND HYGIENE LEGISLATION
5. **SPECIAL SECTION E**: OFFENSES IN THE FIELD OF INDUSTRIAL PROPERTY AND COPYRIGHT OR DISRUPTION OF COMPETITION
6. **SPECIAL SECTION F:** COUNTERFEIT MONEY AND COUNTERFEIT DISTINCTIVE SIGNS
7. **SPECIAL SECTION G**: CYBERCRIME AND ILLEGAL DATA PROCESSING
8. **SPECIAL SECTION H**: ORGANIZED CRIME
9. **SPECIAL SECTION I:** INCITEMENT TO REFRAIN FROM MAKING STATEMENTS OR TO MAKE FALSE STATEMENTS TO THE JUDICIAL AUTHORITY
10. **SPECIAL SECTION L:** ENVIRONMENTAL OFFENSES
11. **SPECIAL SECTION M:** TRANSNATIONAL CRIMES
12. **SPECIAL SECTION N:** OFFENSES RELATED TO IMMIGRATION

The Model was structured in this manner to ensure more effective and streamlined revision operations. Indeed, if the General Section describes the principles of law which are basically fixed, Special Sections are instead periodically revised, given their specific contents.

In addition, changes in the Company and the evolution of legislation – including, for instance, a possible expansion of the types of offense that are included or connected to the scope of application of Leg. Dec. 231/2001 – may result in the need to supplement the Model.

In light of the foregoing, the Surveillance Committee is responsible for adopting any type of measure to cause the board of directors of the Company, or a duly empowered committee, to introduce revisions and supplements, as necessary from time to time.

5.4.1 THE ORGANIZATION AND AUTHORIZATION SYSTEM

The Organization System

The Organization System is sufficiently formalized and clear especially with respect to the assignment of responsibilities, hierarchical reporting lines and descriptions of tasks, and it expressly sets out control principles. The organization structure of the Company was formalized and is graphically reflected in an organization chart, which clearly defines hierarchical reporting lines and functional connections between the different positions of the structure.

The Authorization System

As recommended by the Guidelines, powers to authorize and to sign are granted consistently with organization and operating responsibilities, and, where necessary, there is an accurate indication of thresholds for the approval of expenses, especially in connection with activities that feature the risk of an offense.

5.4.2 CONTROL PRINCIPLES

With this Model, the Company intends to see to the implementation process of the control system centered on the principles described below, as required by the Guidelines.

In connection with each identified sensitive area featuring the risk of an offense, the Company must verify that specific protections are in place.

The following control principles must inspire the management of all sensitive areas disclosed and contained in the so-called map of risks, as well as all corporate processes:

- Ensure integrity and ethics in doing business, by setting out appropriate rules of conduct aimed at regulating all activities which features the risk of offenses;
- Officially define the tasks and responsibilities of each corporate function involved in risk-featuring activities;
- Assign decision making responsibilities commensurately to responsibilities and authority;
- Correctly define, assign and disclose powers to authorize and to sign, and, where necessary, give an accurate indication of thresholds for the approval of expenses, so that no one may be granted unrestricted discretionary powers;

- Ensure the principle of segregated tasks in in managing processes/activities, assigning the crucial phases of the process/activity to different persons and, specifically the following phases:

  - authorization;

  - performance;

  - control;

- Regulate risk-featuring activities with specific procedures, and set appropriate check points (audits, reconciliations, etc.);

- Ensure that each transaction may be audited, is documented, is consistent and appropriate. To such effect, traceability of activities must be guaranteed with appropriate supporting documentation which may be audited at any time. So, in each transaction, the following elements must be easily identifiable:

  - who authorized the transaction;

  - who materially performed it;

  - who recorded it;

  - who audited it.

  Traceability of transaction is ensured to a greater degree of certainty by using IT systems;

- Ensure that records are kept of audits; to such effect, procedures for conducting audits must make it possible to trace back completed audit activities so as to allow to assess that adopted methods are consistent and results are correct. These control principles were taken as reference in the development of corporate procedures.

5.4.3 THE CASH FLOW MANAGEMENT SYSTEM

Art. 6, par. 2, lett. c) of the Decree states that organization, management and control models must comprise “methods to manage financial resources capable of preventing perpetration of offenses”. The rationale to this provision is that many predicate offenses may be committed through company cash flows (e.g.: creating provisions off the books for bribery). The Guidelines recommend to adopt mechanisms for the proceduralization of decisions that document and keep record of the different phases of the decision-making process and make them verifiable and accordingly prevent improper management of such cash flows. Always based on the principles in the Guidelines, the

control system of administrative processes and, specifically, the cash flow management process, is based on the segregation of tasks in the key phases of the process. Segregation must be appropriately formalized and a good level of traceability must be in place for documents and authorization levels associated to each transaction. Namely, specific control elements are:

- several parties operating in the different phases/activities of the process;
- preparing and authorizing the proposal to perform a duly formalized obligation;
- controlling that payments are actually made;
- reconciling after completion;
- several authorization levels for payment requests that are structured based on the amount and the (ordinary/extraordinary) nature of the transaction;
- systematically reconciling internal accounts and banks accounts with accounting records;
- traceability of the steps and single phases of the process which require specific attention with respect to the exhaustive circulation of documents that already originated a payment.

5.4.4 GENERAL PREVENTION PRINCIPLES AND POLICIES

General Prevention Principles

The policy system for the prevention of offenses – as prepared by the Company based on the indications in the Guidelines and best practices – was developed by applying to each sensitive activity the General Prevention Principles listed below, that inspire the General Prevention Policies in the following paragraph as well as the Specific Prevention Polices in each Special Section:

- Regulations: the existence of company regulations and formalized procedures appropriate to serve as conduct principles and operating procedures to perform sensitive activities, and procedures for filing significant documentation. Specifically, CONBIPEL developed specific procedures regulating the management of major sensitive activities. The procedures are an integral part of this Model.
- Traceability: all actions and transactions connected with a sensitive activity must be supported, where possible, by appropriate documents and it must be possible to review ex post the decision-making process, authorization and performance, including through appropriate supporting documents.

- Segregation of tasks: application of the principles of segregation of tasks between who authorizes, who performs and who audits. This segregation is guaranteed by participation of several parties in a single broad corporate process to ensure independence and objectivity in processes.

- Powers of attorney and delegations of powers: granted powers to authorize and to sign must be: consistent with assigned organization and management responsibilities, with the indication, where necessary, of expense approval caps; clearly defined and known within the Company. Any corporate roles vested with the power to commit the Company for specific expenses must be clearly defined, with the indication of the nature of disbursements and their caps. The instrument granting functions must comply with any statutory requirements (e.g. occupational health and safety powers).

General Prevention Policies

In connection with sensitive activities identified for each type of offense (see the Special Sections of the Model), Prevention Polices provide that:

a) All operations, as well as the making and implementation of the Company's decisions must be consistent with the principles and requirements of the law, the articles of association and the bylaws, the Code of Ethics, and any already existing corporate procedures;

b) Company instructions appropriate to provide conduct principles and operating methods to perform sensitive activities must be defined and appropriately disclosed, and the same applies to record keeping procedures applicable to relevant documents;

c) With reference to all operations:

   - Management, coordination and control responsibilities within the business, hierarchical reporting levels and the description of relevant responsibilities must be formalized;

   - Phases that lead to forming the actions and relevant authorization levels must be supported by documents and reconstructible at all times;

   - The Company must adopt all tools to disclose granted powers to ensure knowledge within the Company;

   - Powers granted and exercised in a decision-making process must be consistent with roles and responsibilities and with the significance and/or critical nature of underlying business operation;

- access to the Company's data must be in compliance with EU Regulation no. 2016/679, GDPR, as subsequently amended and supplemented;
- access to and processing of Company's data must be allowed only to duly authorized persons;
- confidentiality in transmitting information must be ensured;
- documents on how decisions are taken and their implementation must be filed and record must be kept, by the relevant function, in a manner that prevents subsequent modification, unless record of such modification is also kept;
- access to already filed documents must be allowed only by authorized people according to internal regulations;

d) With reference to each of the processes involving the sensitive activities listed in this Model and its Special Sections, identify a Process Holder. Specifically, Process Holders:

- Are officially recognized in the organization system of the Company (e.g. internal delegation of powers, job descriptions, procedures), in compliance with any requirements of effectiveness set by the law for the instrument granting functions (e.g. delegation of powers of occupational health and safety);
- Are vested with all the necessary powers to pursue internal objectives to the process, in compliance with the timing and principles that govern it;
- Have full visibility on all the process and (direct or indirect) and access to all relevant information.

Moreover, Process Holders have specific responsibilities to:

- Ensure that the process is completed pursuant to internal regulations (e.g. corporate procedures) and applicable legislation;
- Ensure that the entire process is completed in compliance with the principles of full disclosure and traceability, according to which all transactions must be appropriately supported by documents;
- Inform the Surveillance Committee when they detect anomalies or when critical situations occur (e.g. breaches or suspected breaches of the Model and the Code of Ethics, cases of ineffective, inappropriate and difficult application of control policies).

5.5 REVISING AND ADAPTING THE MODEL

The Board of Directors resolves to revise the Model and adapt it based on amendments and/or supplements which should prove necessary further to:

- Significant breaches of the Model;
- Changes in the internal setup of CONBIPEL and/or of how the Company's operations are performed;
- Changes in legislation;
- Outcome of audits;
- Determination of serious events that are relevant for criminal law purposes even if committed before approval of the Model.

The Board of Directors has exclusive responsibility in this respect.

After approving changes and instructions for immediate application, these are communicated to the Surveillance Committee that, in turn, will immediately make such changes effective and see to the proper disclosure of contents inside and outside CONBIPEL.

The Chairman of the Board of Directors is responsible for periodically introducing any changes to the Model that involve merely descriptive issues, and to timely inform the Board and the Surveillance Committee. The Board has to ratify such changes in its first meeting thereafter. The expression "merely descriptive issues" means elements and information that do not affect the substance of the Model's Special Sections and/or that derive from CONBIPEL's Bodies (such as, for instance changes to the bylaw s, etc.) or specifically empowered corporate functions (such as the redefinition of the organization chart, etc.).

The Model is, in any event, revised periodically and at least on a three-year basis.

6. ORGANIZATION, ADMINISTRATION AND ACCOUNTING ISSUES OF ACTIVITIES AND OPERATIONS

6.1 INTRODUCTION

The business[7] of CONBIPEL S.p.A. is:

1. The manufacture and wholesale and retail of clothing of any kind for men, women, children, and related accessories, and underclothes and homeware and body care products;
2. Wholesale and retail of food, serving food and beverage through the operation of cafés, restaurants and company canteens, and any other service activity howsoever connected to the core business;
3. Construction, trade, management and maintenance of real estate property.

To pursue the corporate business, the Company may, as a sideline:

a) Carry out any commercial, industrial and financial transaction and any transaction on real estate or movable property, necessary or simply useful to achieve the corporate business, including the acquisition of interests in other companies and consortiums, of any type and object, receiving loans by accepting mortgages, giving real and personal guarantees.

The following activities are performed at the registered office:

1. Wholesale and retail of men, women and children clothing, and related accessories, and underclothes, homeware and body care products;
2. Serving food and beverage through the operation of cafés, whose management is outsourced;
3. Management and maintenance of real estate property.

6.2 ORGANIZATION STRUCTURE

The Company's organization chart shows a structure divided into units of staff[8].

In such structure, functions report hierarchically to the CEO or to Managers that are part of the organization structure.

The organization structure of the Company is oriented to ensure the segregations of tasks, roles and responsibilities between operating and control functions and the maximum possible efficiency.

The HR manager is responsible for verifying the organization chart and formalizing it in a constantly up-to-date internal document (Organization Charts).

[7] Chamber of Commerce report on the Company.
[8] Organization chart.

The HR manager, together with the CEO, is also responsible for verifying delegations of powers and proxies to ensure that they are consistent and up to date.

The HR manager prepares and revises job descriptions (indicating function, reporting line, role, responsibility).

6.2.1 THE ORGANIZATION STRUCTURE FOR OCCUPATIONAL HEALTH AND SAFETY

In the area of occupational health and safety, the Company implemented an organization structure that is consistent with applicable provisions on prevention, with a view to eliminating or, where this is not possible, reducing – and accordingly managing – work risks for workers and third parties.

The structure includes the employer, executives, supervisors, managers and staff of the prevention and protection service (hereinafter, also 'RSPP' and 'ASPP', respectively), first aid staff (hereafter also 'APS'), fire-prevention staff (hereafter also 'API'), workers' safety representatives (hereafter also 'RLS'), the company physician, workers, external contractors that carry out activities that are relevant for Occupational Health and Safety, or: a) persons that are assigned a job under a services or works contract; b) manufacturers and suppliers; c) project engineers of work sites and stations and plants and systems; d) fitters and assemblers of systems, work equipment, or other technical tools.
Tasks and responsibilities of these players are formalized consistently with the functional and organization chart of the Company, especially with reference to specific positions in this area.
In defining organization and operating tasks in company management, executives, supervisors and workers, the Company expressly states tasks related to safety operations for which they are responsible, and responsibilities connected to the exercise of such operations, especially in the case of the roles of RSPP, ASPP, RLS, APS, API, and company physician.

6.2.2 THE ORGANIZATION STRUCTURE IN THE AREA OF ENVIRONMENT

In the area of the environment, the Company implemented organization structures that are consistent with the provisions of applicable provisions, with a view to removing or, where this is not possible, reducing – and accordingly managing – environmental risks.
Environment involves:

- The Employer ("DL") as defined in Leg. Dec. 81/2008, that retains the following responsibilities that cannot be delegated:
    - Ensuring that risk assessment is conducted in all stores, pursuant to statutory requirements;
    - Assessing risks related to chemical substances and implementing relevant preventive measures capable of ensuring safety conditions at work for all employees and reduce the risks for CONBIPEL's neighbors;

- The executive with authority over safety ("DS"), under specific delegation of powers and proxies. Duties, as stated in the proxy, may include:
  - Ensuring consistency with environmental regulations in all operations with a view to reduce environmental impact, professional diseases and occupational accidents;
  - Ensuring training to all CONBIPEL employees on all risks;
  - Implementing preventive and corrective actions in line with the Action plan, within the annual budget;
  - Ensuring appropriate relations with trade union representative and, as required by Italian law, official meetings with the RLS.

CONBIPEL does not have an integrated Environmental Authorization ("AIA").

The tasks and responsibilities of the roles described herein are formalized:

- consistently with the functional and organizational chart of the Company;
- consistently with contract clauses (consultants, external contractors, Partners, Service Companies).

In defining organization and operating tasks of company management, executives, supervisors and workers, the Company expressly states tasks related to the environment that they are responsible for.

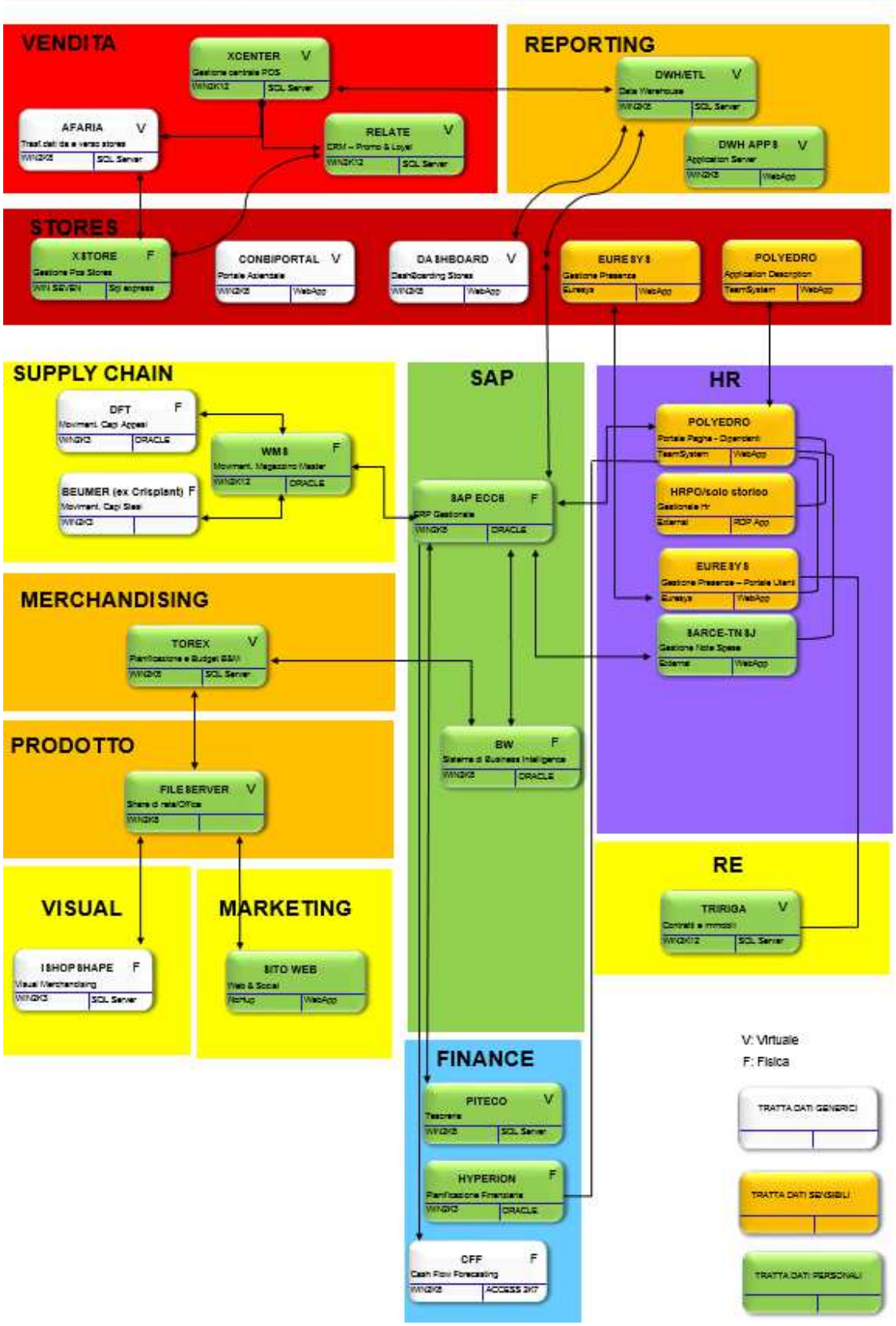
6.3 MANUAL AND AUTOMATED PROCEDURES

In its organization system, CONBIPEL S.p.A. developed a set of manual and automated polices/procedures governing the performance of corporate operations, in compliance with the principles in the Guidelines.

Policies / procedures form the rules that need to be followed in the relevant corporate processes, and they may also include audits to ensure that operations are performed correctly, effective and efficiently.

With specific reference to IT Systems, procedures and applications, the Company implemented a complex architecture of IT systems, which are also interconnected, that governs and regulates traceability, proper access by profile (i.e. the "authority" to access enabled functionalities) and, where applicable, segregation, thus ensuring the running of the process. The following chart reflects the "Applications Map", meaning all IT systems, their interconnection and their classification by Corporate function / Site.

Conbipel APPLICATIONS MAP



Department and administration applications

These are solutions supporting corporate processes outside ERP. These are typically commercial packages that run on windows or web platforms. The0079 increase individual and corporate productivity and streamline Group compliance by managing documents and approval (workflow).

7. SENSITIVE PROCESSES

The review of risks conducted for the purposes of Leg. Dec. 231/2001[9] disclosed Sensitive Processes related to the offenses referred to in the Decree and namely:

a) Offenses committed in relations with Government Agencies (art. 24 and art. 25 of the Decree);
b) Corporate crime under art. 25 ter of the Decree (including private-to-private corruption and incitement to private-to-private corruption);
c) Receiving, laundering and using cash, assets or benefits of a criminal origin, and self-laundering (art. 25 octies of the Decree);
d) Offenses in art. 25 septies of the Decree, offenses related to occupational health and safety (art. 25 septies of the Decree);
e) Offenses related to industrial property and copyright and the disruption of competition (art. 25-bis, 25-bis1 and 25-novies of the Decree);
f) Offenses related to counterfeit money, securities, tax stamps and distinctive signs (art. 25 bis of the Decree);
g) Cybercrime and illegal data processing (art. 24-bis of the Decree);
h) Organized crime (art. 24 ter of the Decree);
i) Incitement to refrain from making statements or to make false statements to the judicial authority (art. 25-decies of the Decree);
l) Environmental offsets (art. 25-undecies of the Decree);
m) Transnational crime;
n) Immigration-related offenses (art. 25-duodecies of the Decree).

The specific dedicated chapters of this Model called “Special Sections” describe (a) in detail sensitive processes in connection with each of the category of crimes listed above and (b) their regulations.

Risks connected to organized crime (art. 24 ter Leg. Dec. 231/2001) and incitement to refrain from making statements or to make false statements to the judicial authority (art. 25 decies D Leg. Dec. 231/2001) are regulated not only by the principles in the Code of Ethics adopted by the Company but also in specific special sections, even if they may only hypothetically be envisaged.

Since the Company, its parent company and its subsidiary are not listed on any regulated stock market, risks connected to market abuse and market manipulation (art. 25-sexies Leg. Dec. 231/2001) do not materially subsist.

Risks connected to Offenses against individuals (arts. 25 quater1 and quinquies Leg. Dec. 231/2001) and Racism and xenophobia (art. 25-terdecies of the Decree) may only hypothetically and not materially be envisaged.

[9] Also refer to the table of risk analysis by offense.

8. THE SURVEILLANCE COMMITTEE (SC)

8.1 IDENTIFYING THE SURVEILLANCE COMMITTEE

Based on the provisions of the Decree (art. 6, para. 1, lett. a) and b)), the entity may be released from the liability resulting from perpetration of offenses by its qualified parties (under the Decree), if the board of directors, among other things, engaged a committee with independent powers of initiative and control to constantly monitor operation of and compliance with the model; the committee must feature the following requisites (as recommended by the Guidelines):

- ***autonomy and independence;***
  - no conflict of interests, including potential conflicts, with CONBIPEL;
  - autonomous powers of initiative and control;
  - no operating tasks within CONBIPEL;
  - reporting directly to the BoD;
  -
- ***professionalism*** meaning:
  - adequate specialist skills;
  - specialist techniques and tools to be able to complete tasks, including through the advice of external parties;

- ***continuity of action*** meaning:
  - term of appointment unrelated to the term of other corporate bodies;
  - periodic audits.

8.2 ESTABLISHMENT, APPOINTMENT AND REPLACEMENT OF THE SC

The Surveillance Committee (hereinafter also "SC") of CONBIPEL is established by BoD resolution and holds office for the term that is set upon its appointment. It may comprise one or more members. The SC leaves office on the date set upon its appointment, even if it continues to carry out its functions temporarily until appointment of a new SC. The BoD has the authority to call a meeting with the SC at any time.

Appointment as a member of the SC is conditional on meeting the personal requisites of honorability, integrity and respectability, and on the lack of causes of incompatibility with the appointment, and of potential conflicts of interest with the role and duties that one would carry out. Accordingly, upon granting the engagement, persons designated to fill the office of member of the SC are required to deliver a statement in which they attest that there is no reason of incompatibility, as listed in the previous paragraph. These rules also apply when a member of the SC is replaced.

Revocation of the powers and granting to other parties may occur upon natural expiration of the term of office or only for just cause, including when such cause is connected to a reorganization of the Company. Revocation is implemented by a specific resolution of the BoD. "Just cause" for revoking the powers connected to the appointment as member of the SC includes but is not limited to:

- Gross negligence in performing the duties connected to the engagement: failure to draft the annual recapping report on completed activities, failure to draft the surveillance plan;
- "failure to surveil or insufficient surveillance" by the SC – pursuant to art. 6, par. 1, lett. d), Decree – established by a court decision, including if an appeal is still admissible, delivered against CONBIPEL under the Decree or a court decision of application of the sentence upon request (so-called plea-bargaining);
- In case of an internal member, granting operating responsibilities and functions within the company organization that are incompatible with the core requisites of "autonomy and independence" and "continuity of action" of the SC. In any case, any available organization measure involving internal members (such as termination of employment, deployment to a different job task, dismissal, disciplinary measures, appointment of a new manager) must be reported to and acknowledged by the BoD;
- In case of an external member, serious and verified reasons of incompatibility which invalidate independence and autonomy;
- Failure to meet even only one of the requisites for eligibility.

Any decision involving individual members or the entire SC concerning removal or replacement are exclusively reserved for the BoD.

8.3 FINANCIAL RESOURCES ALLOCATED TO THE SURVEILLANCE COMMITTEE

Every year, the BoD allocates a budget to the SC based on the latter's requests.

Allocation of the budget allows the SC to operate independently and with appropriate tools to effectively complete the duties that are assigned to it by this Model, pursuant to the Decree.

8.4 FUNCTIONS AND POWERS OF THE SURVEILLANCE COMMITTEE

In performing its duties, the SC will have, under its direct supervision and responsibility, the cooperation of all the Company functions and facilities, or external consultants. This enables the SC to ensure a high level of professionalism and the necessary continuity of action.

The SC has independent powers of initiative, action and control, which cover all segments and functions of CONBIPEL and need to be exercised to timely and effectively carry out the functions described in the Model and in its implementing regulations.

Specifically, the SC is vested with the following powers and duties to implement and perform its functions:

- Monitor operation of the Model with respect to both prevention of the offenses in the Decree and the ability to bring light on any actually perpetrated unlawful conduct;
- Carry out periodic audits and checks, on an ongoing basis – on the time-basis and with the procedures defined in the surveillance activity plan – and sample checks, based on the various areas of action or types of activity and their critical points to determine the Model's efficiency and effectiveness;
- Have unrestricted access to any department and unit of CONBIPEL – with no need for any prior approval – to ask for and receive information, documents and data regarded as necessary to carry out the duties in the Decree, from all executives and staff. If a reasoned denial to access documents is made, the SC will draft a specific reasoned report for the BoD, where it does not agree with such denial;
- Ask for significant information or ask to be shown documents, including IT documents, related to risk-featuring activities, from Directors, control bodies, the independent auditor, independent contractors, consultants and in general all parties required to comply with the Model;
- See to, develop and promote the constant update of the Model, submitting proposals, where necessary, to the management for any appropriate revision and adjustment that should prove necessary as a consequence of: i) significant breaches of the Model's regulations; ii) significant changes in the internal setup of CONBIPEL and/or of how the Company's business in is operated; iii) changes in legislation;
- Monitor compliance with the Model's requirements, in connection with the different types of offenses in the Decree and any subsequent legislation which expanded its scope of application, verify compliance with the procedures in the Model and detect any discrepant conduct possibly disclosed by the analysis of information flows and reports that it received;
- Ensure the periodic revision of the mapping and identification of sensitive areas;
- Maintain relations with the independent auditor and with other consultants and independent contractors involved in implementing the Model;
- Liaise and ensure information flows with the BoD;
- Promote disclosure and training sessions on the contents of the Decree and the Model, on the impact of regulations on the Company business and on

rules of conduct, setting up frequency checks and possibly differentiated plans for people that work in the different sensitive areas;
- Verify the setup of an effective internal communication system to allow transmission of information that is significant for the purposes of the Decree (whistleblowing) ensuring protection and confidentiality of the person making the report;
- Give explanations on the meaning and application of the Model;
- Develop and submit to the BoD the budget needed to properly perform the duties assigned to it in a fully in independent manner. The SC may autonomously commit resources that exceed its powers of disbursement when such resources are necessary to face exceptional and urgent situations. In these events, the SC must inform the BoD at first meeting after the event;
- Report without delay to the management body, for the adoption of appropriate measures, any established breaches of the Model that could trigger any liability for CONBIPEL;
- Promote the activation of any disciplinary procedures and propose the penalties, if any, described in Chapter 7 of this Model;
- Verify and assess if the disciplinary system is appropriate pursuant to and for the purposes of the Decree.

8.5 REPORTING OF THE SC TO THE COMPANY TOP MANAGEMENT

The SC reports on the implementation of the Model and the detection of any critical issues.

The SC has three reporting lines:

1. The first line, on an on-going basis, to the CEO that the SC shall address immediately, by a report, anytime (a) an issue or critical element should emerge involving a sensitive area under Leg. Dec. 231/2001, (b) breaches of the Model are committed, (c) changes in legislation on the administrative liabilities of bodies corporate are introduced, (d) amendments to the Model prove necessary or appropriate, etc.;
2. The second line, on a periodic basis, every six months, to the Board of Directors and the Board of Statutory Auditors, to whom the SC will send a written report on its activities (indicating specifically the controls and audits it made, their outcome, the revision, if any, of the mapping of Sensitive Processes, the degree of cooperation of all corporate functions involved from time to time, and relations with the controlling shareholder and any other supervisory body or authority; an action plan for the following year);
3. The third line, on an occasional basis, as necessary, to the Board of Statutory Auditors when the breach involves top managers of the Company and the Board of Directors.

If the SC detects critical issues relating to the persons to whom it reports, the relevant report will have to be addressed without delay to one of the other entities listed above.

Reporting concerns:

a) The activity carried out by the SC;

b) Any critical issues (and tips for improvement) emerged in terms of conduct or internal events, and in terms of the Model's effectiveness.

Meetings with the bodies to which the SC reports must be recorded in appropriate minutes, copy of which will be kept by the SC pursuant to the bylaws and its regulations.

The Chairman of the BoD, the CEO and the Chairman of the Board of Statutory Auditors have the authority to call the SC at any time, through its Chairman, who, in turn, has the authority to ask, through the relevant functions or entities, that the bodies listed above be called for urgent matters.

8.6 INFORMATION FLOWS

The Surveillance Committee, including through the definition of a procedure, may determine the type of information that managers involved in managing sensitive activities are required to transmit together with the method and time-basis to forward such reports to the SC.

The corporate functions involved in sensitive activities are required to transmit the following information to the Surveillance Committee:

- Periodic results of any control activities that they perform pursuant to the Model, including upon request (reports recapping activities, etc.);

- Any anomaly or inconsistency detected in available information.

Information includes but is not limited to:

- Operations that fall under sensitive activities (for instance: periodic recapping reports on agreements with government entities, information on new hires or use of financial resources to purchase goods or services or other investment activities, etc.);

- Measures and/or information from the criminal investigation department or from any authority, which disclose that investigations are in progress, including, against John Doe, for offenses covered by the Leg. Dec. 231/2001 and which could involve CONBIPEL;

- Requests for legal assistance submitted by employees in the event of legal proceedings started against them in connection with the offenses covered by the Decree, unless expressly prohibited by the judicial authorities;
- Reports prepared by managers of company functions in the course of their control activity which could disclose facts, actions, events or omissions with a potentially critical impact with respect to compliance with the Model's provisions and regulations;
- Information on disciplinary procedures and resulting penalties, if any, (including measures adopted against employees) or dismissals of such procedures along with the relevant reasons;
- Any other information which, although not included in this list, is significant for the purposes of proper and full surveillance and revision of the Model.

In any event, the SC defines and discloses a detailed chart of Information Flows destined to it.

Information flows are sent to the SC by transmitting the documents to the dedicated email account.

8.6.1 WHISTLEBLOWING

The obligation to report any conduct which is contrary to the provisions of the Model falls under the more general due diligence and loyalty obligations of employees. External consultants or independent contractors and similar are under the contractual obligation to immediately report any circumstance where they directly or indirectly receive from an employee/representative of CONBIPEL a request for conducts which could trigger a breach of the Model.

Therefore, all the Company staff, whether Top Managers or Subordinate employees, and all external parties that are Addressees of this Model are required to communicate directly with the Surveillance Committee to report the perpetration of any offenses, circumstances involving unlawful conducts under the Decree and grounded on specific and consistent elements of fact, any breaches of the Model, and any episode which departs from the conduct principles in the Model and in the Code of Ethics, which they became aware of in carrying out their functions. Communication may occur through several alternative channels appropriate to ensure, with IT means, confidentiality of the identity of the whistleblower, pursuant to art. 6, par. 2 bis, lett. b) of the Decree.

<u>Contents of the report</u>

For the purposed described above, whistleblowers are required to provide all elements known to them, useful to verify reported facts, through appropriate checks. Specifically, reports must contain the following essential elements:

Subject: a clear description of the facts that are being reported is required, along with the indication of circumstances (where known) of time and place where the facts were committed or omitted.

Reported individual: the whistleblower must indicate the description or in any event any other elements (such as the function/role in the Company) which allows to easily identify of the alleged author of the misconduct.

Moreover, whistleblowers may indicate the following additional elements: (i) their identification details, where they do not intend to keep their identity confidential; (ii) indication of any other persons that may report on narrated events; (iii) indication of any documents that may confirm the substance of the facts.

The contents of reports, even where anonymous, must always be relevant to the Decree. Anonymousness cannot howsoever be a tool to voice frictions or contrast between staff members. Likewise, it is forbidden to:

- Use abusive language;
- Make reports with merely disparaging purposes;
- Make reports which concern solely private life, with no direct or indirect connection with corporate business. These reports shall be regarded as even more improper when they refer to sexual, religious, political and philosophical beliefs.

In In short, all reports must serve the sole purpose of protecting the integrity of the Company or preventing and/or fighting against misconducts as defined in the Model.

Communication channels

The communication channels with the Surveillance Committee described below, in accordance with whistleblowing regulations, ensure confidentiality and protection of the whistleblower including from any retaliation. The Company also monitors that any career advances of whistleblowers are not treated with discrimination, and punishes with disciplinary measures based on the seriousness of facts, and in compliance with the criteria in Chapter 10 of the Model, whistleblowers that report – acting with willful intent or with serious negligence - facts that prove to be unfounded.

Communication channels are:

Registered letter: registered letter addressed to the Chairman of the SC, Mr. Paolo Baruffi, at the following address: Paolo Baruffi, c/o Carnelutti Studio Legale Associato, Via P. Amedeo 3, Milano 20121. The envelope must clearly bear the wording "*Strictly confidential. 231 disclosure by an employee*" to ensure the utmost confidentiality.

Email account: *odv@conbipel.it*; to such effect, the Company guarantees that only the SC has access to this account; specifically, no one, including system administrators, has the possibility of accessing, checking or disclosing the contents of the above email account. Breach of this prohibition triggers the application of disciplinary penalties.

Treatment of reports

The Surveillance Committee adopts the most appropriate measures to ensure confidentiality of the identity of those who report information to the SC. However, conducts aimed solely at slowing down the activity of the Surveillance Committee must be appropriately punished. The Company guarantees whistleblowers in good faith from any form of retaliation, discrimination or unfavorable treatment and, in any event, confidentiality of the identity of the whistleblower is ensured, without prejudice to the protection of the rights of the Company or of persons that are accused incorrectly or in bad faith.

For the above purposes, the Surveillance Committee collects and stores the reports that it receives in a dedicated (IT and/or hardcopy) file which may be accessed only by members of the SC. The Surveillance Committee at its sole discretion and under its own responsibility considers the reports that it receives and the cases where it needs to take action. Its decision on the outcome of the assessment must be reasoned in writing.

9. TRAINING RESOURCES AND DISSEMINATING THE MODEL

9.1 KNOWLEDGE BY AND TRAINING TO EMPLOYEES AND COMPANY BODIES

With a view to an effective implementation of the Model, the Company intends to ensure proper knowledge of the rules of conducts in the Model by staff already working for the Company and future hires, with a different level of insight based on the different level of involvement of resources in Sensitive Processes.

The disclosure and training system is under the supervision and supplemented by the activity carried out in this area by the SC together with the HR manager and with the managers of other functions involved in applying the Model from time to time.

- **Initial disclosure**

Adoption of this Model is disclosed to all resources present within the Company at such time.

Instead, new hires and persons that have corporate positions for the first time receive an information kit (e.g. Code of Conduct, CCNL, Model, Leg. Dec. 231/2001, etc.), with which they are guaranteed knowledge of elements that are considered of primary importance.

- **Training**

The contents and procedures for training aimed at spreading knowledge of regulations in Leg. Dec. 231/2001 vary depending on the title of the Addressees, the level of risk of the area where they operate, whether they have Company representation functions.

Specifically, the Company defined different levels of knowledge and training through appropriate disclosure tools for:

1. Top management, members of the SC and of Corporate Bodies;
2. Employees that operate in sensitive areas;
3. Employees that do not operate in sensitive areas.

All training programs have a basic common content consisting in illustration of the principles in Leg. Dec. 231/2001, major elements forming the Organization, management and control Model, individual offenses regulated by Leg. Dec. 231/2001, and conducts regarded as sensitive in connection with the offenses described above.

In addition to this common basis, each training program is adjusted to give its users the necessary tools to fully comply with the Decree in connection with the respective scope of operations and tasks of the addressees of the program.

Taking part in the training programs described above is required and the SC is in charge of verifying actual attendance.

The SC is also responsible for controlling the quality of the training programs described above.

The provider of training services is required to retain objective records of the training sessions it gave in a specific file, which it will be required to store.

9.2 DISCLOSURE TO CONSULTANTS AND PARTNERS

Consultants and Partners are incomed of the contents of the Model and of the Company's need that their conduct be compliant with the provisions of Leg. Dec. 231/2001, as per the procedural rules.

10. DISCIPLINARY SYSTEM

10.1 FUNCTION OF THE DISCIPLINARY SYSTEM

The definition of a system of penalties (proportionate to breaches and serving as deterrent), applicable in the event of breaches of the rules in this Model and the Code of Conduct, makes the surveillance function of the SC efficient and serves the purpose of ensuring the effectiveness of the Model.

The definition of this disciplinary System is, under art. 6, par. 1, letter e), of Leg. Dec. 231/2001, an essential requisite of the Model to release the Company from liability.

CONBIPEL S.p.A. has, thus, adopted a disciplinary system (hereinafter also "Disciplinary System") aimed to punish **breaches of the principles, the rules and the measures in the Model and in the relevant Policies**, in compliance with the provisions of national collective bargaining agreements and applicable laws and regulations.

Penalties apply to any breaches of the Model and relevant Policies committed by "top" managers and persons under the management of others or operating in the name and/or on behalf of CONBIPEL S.p.A.

The application of the disciplinary system and relevant penalties is unrelated to the completion and outcome of any criminal proceedings started by the judicial authorities in the event that the punishable conduct is also an offense relevant for the purposes of Leg. Dec. 231/2001.

The Company's right to apply the penalties set out by applicable laws and by corporate practice with reference to conducts that are not relevant for the application of Leg. Dec. 231/2001 is unaffected.

10.2 STRUCTURE, DEVELOPMENT AND ADOPTION OF THE DISCIPLINARY SYSTEM

A separate document was prepared to regulate this aspect comprehensively, whose content fully coincides with this chapter and which forms an integral part of the Model.

The Disciplinary System is posted in a place accessible to all so that full knowledge by all Addressees is guaranteed. It is also delivered, in hardcopy or electronical format to key offices and employees and it is published on the Company intranet.

The Disciplinary System comprises the four following sections:

Section I: people that may be punishable

Persons to whom penalties apply are listed, divided into four different categories:

1) Directors and Auditors;

2) other Top Managers;

3) Employees;

4) Service Companies, Consultants, Partners.

Section II: potential breaches

Breaches that are relevant from a disciplinary perspective are specified and classed into five different categories based on an order of increasing seriousness:

A) Breach of the Company's internal procedures/policies as set out in the Model (for instance, failure to comply with required procedures, omitted reports to the SC of required information, omitted controls, etc.) or adoption, in performing activities connected to Sensitive Processes, of conducts that do not comply with the operating instructions or procedures of the Company or the requirements of the Model or the Code of Conduct;

B) Breach of the Company's procedures/policies as set out in the Model or adoption, in performing activities connected to Sensitive Processes, of conducts that do not comply with operating instructions or procedures of the Company or the requirements of the Model or the Code of Conduct, capable of exposing the company to an objective situation featuring the risk of perpetration of one of the Offenses;

C) Adoption, in performing activities connected to Sensitive Processes, of conducts that do not comply with operating instructions or procedures of the Company or the requirements of the Model or the Code of Conduct and aimed unambiguously at perpetrating one or more Offenses;

D) Adoption, in performing activities connected to Sensitive Processes, of conducts that are clearly in breach of the operating instructions or procedures of the Company or the requirements of the Model or the Code of Conduct, capable of triggering the actual application against the Company of the penalties in Leg. Dec. 231/2001;

E) Perpetration of one of the Offenses.

The section also indicates breaches in the area of occupational health and safety that are relevant for disciplinary purposes, which are classed in four different categories based on an order of increasing seriousness:

F) Failure to comply with the Model, when the breach triggers a situation of actual danger for the safety of one or more people, including the perpetrator of the breach, and provided that one of the conditions in items G, H and I is not met;

G) Failure to comply with the Model, when the breach determines damages to the physical integrity of one or more persons, including the perpetrator of the breach, provided that the one of the conditions in items H and I is not met;

H) Failure to comply with the Model, when the breach triggers an injury that qualifies as "serious" under art. 583, par. 1, of the Criminal Code, to the physical integrity of one or more persons, including the perpetrator of the breach, provided that one of the conditions in item I is not met;

I) Failure to comply with the Model, when the breach triggers an injury that qualifies as "very serious" under art. 583, par. 1, of the Criminal Code, to the physical integrity or triggers the death of one or more persons, including the perpetrator of the breach.

Section III: Penalties and categories of Addressees

Penalties that may theoretically be inflicted on each category of Addressees are listed with respect to all relevant conducts.

Any breach of the rules in this Model or in the Code of Conduct by Service Companies, Consultants or Partners, as applicable to them, and any perpetration of Offenses by them is punished pursuant to specific clauses in the relevant agreements.

Any compensation claim if such conduct results in material damages to the Company, like in the case of application against it by a court of the measures in Leg. Dec. 231/2001, is unaffected.

In any event, the penalties and the compensation claim, if any, are proportionate to the level of responsibility and autonomy of Addressees, the existence of any prior disciplinary precedents against them, the intentional character and the seriousness of the conduct, by this meaning the level of risk which the Company may reasonably consider having been exposed to under Leg. Dec. 231/2001, as a result of such misconduct.

Section IV: disciplinary procedure

The procedure for inflicting and applying penalties is regulated for each category of Addressees, specifying for each one of them:

1) The phase for claiming breach against the relevant person;
2) The counterclaim by the person to whom the breach was claimed;
3) The phase for determining and subsequently applying the penalty.

The disciplinary system is constantly verified and assessed by the SC and by the HR Manager, who retains responsibility for the actual application of the disciplinary measures described herein upon indication, if any, of the SC and after consultation with the reporting manager of the perpetrator of the punished conduct.

Powers already granted to the company management with respect to establishment of breaches, disciplinary procedures and infliction of penalties remain unchanged, with the restriction of the relevant areas of responsibility.

The provisions of the Disciplinary System do not restrict the authority of the Addresses to exercise all their rights, including the rights to dispute and object, through the disciplinary procedure or an Arbitration Panel, granted to them by laws or regulations, and by national collective bargaining agreements or applicable Company regulations.

10.3 MEASURES AGAINST EMPLOYEES

Breaches by Employees whose employment is regulated by collective bargaining agreements applied by the Company of rules of conduct in this Model and in the Code of Conduct are disciplinary breaches.

Penalties applicable against workers that are employed by the Company, pursuant to art. 7 of Law no. 300/1970 (so-called Workers' Statute) and any special regulations possibly applicable, as subsequently amended and/or supplemented, are provided for in the penalty framework of the relevant collective bargaining agreement and namely:

a) Verbal warning;

b) Written warning;

c) Fine, from 1 to 4 hours of work;

d) Suspension from work and remuneration for a period of no more than 10 days;

e) Dismissal for material nonperformance of contract obligations by the worker (justified personal reason under art. 7, Law no. 300 of 20 May 1970 and of the applicable CCNL);

f) Dismissal for serious nonperformance that prevents continuation of employment, including temporarily (just cause).

When so required by the nature of the nonperformance or the need for assessments further to such nonperformance, the Company – pending any resolution on the final disciplinary measure – may order the temporary suspension of the worker from service for the time that is strictly necessary.

All the provisions and guarantees set out in art. 7 of Law no. 300/1970, as subsequently amended and/or supplemented, relating to disciplinary procedures are applicable. Any powers previously granted within the Company in the area of determining breaches, disciplinary procedures and application of penalties remain valid, with the restriction of the relevant delegations and areas of responsibility.

The following conducts are breaches:

1. Workers that commit a slight non-compliance of contract provisions or internal regulation and of rules of conduct or guidelines and instruction given by Top Managers or superiors, and who commit a slight negligence in carrying out their job incur in the measure of a "**verbal warning**";

2. workers that repeatedly breach the procedures with a repetition of nonperformance punishable with a verbal warning incur in a "**written warning**". The same penalty applies to workers that, in carrying out their operations, adopt a conduct that does not comply with the requirements, with a minor noncompliance of contractual provisions or directives or instructions given by

management, or superiors, or adopts a negligent conduct or omits to report or tolerates minor irregularities committed by other staff or third parties;

3. workers who repeatedly breach procedures with a repetition of nonperformance punishable with a verbal warning and with the subsequent written warning incur in a "**fine**".
4. workers who commit acts that, based on objective circumstances, specific consequences or recidivism, are more material than conducts that are punished with minor penalties, incur in "**suspension from work and remuneration of no more than 10 days**". The same penalty applies to workers that, in carrying out their operations, adopt a conduct that does not comply with the requirements adversely affecting the Company or third parties, with the repeated noncompliance of a certain seriousness of contractual provisions or directives or instructions given by Top Managers or superiors, and adopts a conduct of gross negligence or a conduct that adversely affects the Company or third parties, or fails to report or tolerates serious irregularities committed by other staff or third parties;
5. workers who breach internal regulations and rules of conduct, disciplinary contract provisions or duties concerning disciplinary action, the Company's directives, or work performance, capable of being construed, whether for the specific nature of the noncompliance or for recidivism, a "material" nonperformance of related obligations, incur in "**dismissal for material nonperformance of contract obligations by the worker (justified reason)**";
6. workers that adopt a conduct whose seriousness is such (whether for willful intent or criminal or financial consequences or recidivism or specific nature) that it results in the loss of the trust on which employment is based, and that it does not allow to continue employment albeit temporarily incurs in **"dismissal for just cause"**.

The type and extent of each of the penalties listed above, with specific reference to the provisions of Leg. Dec. 231/2001, will be applied by taking into account applicable laws, corporate practice and:

a) willful intent of the conduct or degree of negligence, recklessness, or unskillfulness including by considering the predictability of the event;

b) overall behavior of the worker especially with respect to any disciplinary precedent, to the extent admitted by law;

c) workers' job tasks;

d) functional position of persons involved in the facts forming the nonperformance;

e) other specific circumstances that characterize the disciplinary misconduct.

The Company's right to apply the penalties set out in applicable laws and corporate practice to conducts that are not relevant for the application of Leg. Dec. 231/2001 is unaffected.

To determine recidivism, with specific reference to relevant conducts under Leg. Dec. 231/2001, only disciplinary penalties inflicted in the last two years are taken into account.

The Company's right to claim compensation for any losses resulting from an Employee's breach of internal regulations and policies and of rules of conduct is unaffected.

Claimed compensation, if any, for damages is proportionate to:

a) the level of responsibility and autonomy of the Employee, perpetrator of the disciplinary misconduct;

b) any disciplinary precedents of the Employee;

c) the level of willful intent in the conduct;

d) the seriousness of the effects, meaning the level of risk which the Company reasonably believes it was exposed to as a result of the punished conduct.

Powers already granted to company management with respect to establishment of breaches, disciplinary procedures and infliction of penalties remain unchanged, with the restrictions of the relevant areas of responsibility.

The ultimate person responsible for the practical application of the disciplinary measures described above in the event of conducts that are relevant for Leg. Dec. 231/2001 is the HR Manager together with the CEO who will determine the penalties by also taking into consideration any reports by the Surveillance Committee, based on individual provisions of law (for instance, Leg. Dec. 231/2001, Leg. Dec. 81/2008).

All requirements, in terms of compliance of the disciplinary process in the CCNL and in corporate practice are unaffected.

10.4 MEASURES AGAINST EXECUTIVES

In the event of breaches by executives of the procedures in this Model or adoption, in carrying out activities connected with Sensitive Processes, of a conduct that does not comply with the requirements of the Model or of the Code of Conduct, the Company applies most appropriate measures to perpetrators pursuant to the applicable CCNL for executives and relevant established court decisions.

Any charges and the relevant penalties applied to Executives that are also Top Managers further to breaches of the Model, must be decided by the Board of Directors, after consulting the CEO, notifying the Chairman of the Surveillance Committee, protecting the Company's interests without jeopardizing its image.

10.5 MEASURES AGAINST DIRECTORS

In the event of breach of the Model or the Code of Conduct by one or more members of the Board of Directors, the SC informs the Board of Statutory Auditors and the entire Board of Directors, which consider any appropriate actions including, but not limited to, calling a shareholders' meeting to adopt the most appropriate measures pursuant to the law.

10.6 MEASURES AGAINST STATUTORY AUDITORS

In the event of breach of this Model or the Code of Conduct by one or more of the Statutory Auditors, the SC informs the entire Board of Statutory Auditors and the Board of Directors, which consider any appropriate actions including, but not limited to, calling a shareholders' meeting to adopt the most appropriate measures pursuant to the law.

10.7 MEASURES AGAINST THE MEMBERS OF THE SC

In the event of breach of this Model or of the Code of Conduct by one or more members of the SC, any other member of the SC or any one of the Statutory Auditors or Directors informs the Board of Statutory Auditors and the Board of Directors, which considers the most appropriate measures to adopt including but not limited to, removal from office of the members of the SC that breached the Model and the consequent appointment of new member to replace them, or the removal from office of the entire SC with the consequent appointment of a new one.

10.8 MEASURES AGAINST SERVICE COMPANIES, CONSULTANTS, PARTNERS

Any breach by Service Companies, Consultants or Partners of the rules in this Model or in the Code of Conducts applicable to them or any perpetration of the Offenses is punished according to the specific contractual clauses included in the relevant agreements. The right for the Company to claim compensation for any losses, where caused by such conduct, like in case of application by a court to the Company of the measures in Leg. Dec. 231/2001, is unaffected.

10.9 MEASURES APPLICABLE UNDER WHISTLEBLOWING REGULATIONS

Pursuant to the provisions of art. 2-bis, par. 1, lett. d) of the Decree, the penalties in the previous paragraphs, pursuant to the principles and criteria stated therein, apply to those who breach measures that safeguard whistleblowers, and whistleblowers that make reports with willful intent or serious negligence that turn out to be unfounded.

Specifically, retaliation against whistleblowers in good faith is a serious disciplinary breach that will be punished according to the procedures described in the previous paragraphs. Adopting discriminatory actions against whistleblowers may be reported to the National Labor Inspectorate, for the remedies which fall under its jurisdiction, not only by the whistleblower but also by the trade union indicated by the latter. Retaliating or discriminatory dismissal of the whistleblower is null and void. Changes in job duties as per art. 2103 of the Italian Civil Code are also null and void, as is any other action of retaliation or discrimination adopted against the whistleblower.

In the event of disputes connected to the application of disciplinary measures or downgrading, dismissal, transfers, or other reorganization measure to the whistleblower with direct or indirect negative effects on the work conditions of the latter after submission of a report, the employer bears the burden of proving that such measures were grounded on reasons other than the report.

Any misuse of whistleblowing channels is prohibited. Protection of the identity of the whistleblower no longer applies when reports are clearly unfounded and deliberately aimed at causing harm to the person forming the subject matter of the report or the Company. This conduct as well is a serious disciplinary breach and is punished according to the procedures described above.

Organization, Management and Control Model under Leg. Dec. 231/2001

SPECIAL SECTIONS

SPECIAL SECTION A	OFFENSES IN RELATIONS WITH GOVERNMENT AGENCIES
SPECIAL SECTION B	CORPORATE CRIME
SPECIAL SECTION C e SPECIAL SECTION C-BIS	RECEIVING, LAUNDERING AND USING CASH, ASSETS OR BENEFITS OF A CRIMINAL ORIGIN, AND SELF-LAUNDERING AND CRIMES FOR THE PURPOSES OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER
SPECIAL SECTION D	MANSLAUGHTER AND SERIOUS AND VERY SERIOUS UNINTENTIONAL INJURIES COMMITTED WITH BREACHES OF ACCIDENT-PREVENTION PROVISIONS AND OCCUPATIONAL HEALTH, SAFETY AND HYGIENE LEGISLATION
SPECIAL SECTION E	OFFENSES IN THE FIELD OF INDUSTRIAL PROPERTY AND COPYRIGHT OR DISRUPTION OF COMPETITION
SPECIAL SECTION F	COUNTERFEIT MONEY AND COUNTERFEIT DISTINCTIVE SIGNS
SPECIAL SECTION G	CYBERCRIME AND ILLEGAL DATA PROCESSING
SPECIAL SECTION H	ORGANIZED CRIME
SPECIAL SECTION I	INCITEMENT TO REFRAIN FROM MAKING STATEMENTS OR TO MAKE FALSE STATEMENTS TO THE JUDICIAL AUTHORITY
SPECIAL SECTION L	ENVIRONMENTAL OFFENSES
SPECIAL SECTION M	TRANSNATIONAL CRIMES
SPECIAL SECTION N	OFFENSES RELATED TO IMMIGRATION

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION A
Offenses in Relations with Government Agencies

11. OFFENSES IN RELATIONS WITH GOVERNMENT AGENCIES

11.1 CASES OF OFFENSES IN RELATIONS WITH GOVERNMENT AGENCIES (ART. 24 AND ART. 25 OF LEG. DEC. 231/2001).

This Special Section refers to offenses that may potentially be committed in relations between the Company and Government Agencies.

Each offense is described in articles 24 and 25 of Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

11.2 SENSITIVE PROCESSES IN RELATIONS WITH GOVERNMENT AGENCIES

The following sensitive macro-processes emerged in connection with relations with Government Agencies:

- Handling legal, tax and corporate affairs (i.e. Chamber of Commerce, Court, Register of Companies, Ministry of the Economy, Notaries Public, etc.);
- Obtaining and/or renewing authorizations, permits and licenses (i.e. municipalities, provinces, local authorities, local health units, fire departments, etc.);
- Managing human resources with respect to administrative, social security and welfare issues (i.e. Ministry of Labor, National Social Security Agency (INPS), Workers' Mandatory Insurance Agency (INAIL), Labor inspectorate, Provincial Labor Agency, etc.);
- Inspections, investigations and similar (i.e. Tax Police, DIA – Antimafia Investigation Department, INPS, INAIL, Labor inspectorate, environmental, safety and health officials, etc.);
- Organizing events (i.e. local authorities, artistic heritage agency, Italian Society of Authors and publishers (SIAE), state entities / entities entrusted with a public service, contractual counterparties, etc.);
- Litigation in the areas of civil, criminal and administrative law (i.e. judges, officials of the public prosecution, etc.);
- Disclosing corporate/business data of any nature (i.e. relations with the Italian Data Protection Authority, Competition Authority, etc.);
- Managing relations with government entities to handle accomplishments, audits and inspections connected with the generation of solid, liquid or gaseous waste, or smoke emissions or the generation noise/electromagnetic pollution, inspected by government entities;
- Managing relations with government entities in connections with occupational safety and health (Leg. Dec. 81/2008) and complying with the

precautionary measures in laws and regulations for the employment of staff assigned to specific job duties;

- Managing relations with public entities in connection with hiring staff belonging to categories of protected persons or to whose engagement preferential terms apply;
- Managing the operations to secure and/or administrate contributions, subsidies, funding, insurance or guarantees granted by government entities;
- Managing registered movable property connected to business operations;
- Preparing income tax returns or withholding agents' tax returns or other returns functional to determining and settling taxes in general;
- Setting up, maintaining, updating or managing software of government entities or provided by third parties on behalf of government entities;
- Managing arbitration or legal proceedings;
- Supplying goods and or rendering services;
- Managing payments and financial resources;
- Managing consultancies;
- Managing the staff selection and recruitment process;
- Managing IT security accomplishments.

Involved Company Roles:

- CEO;
- CFO, Treasury Manager, Financial Control, Accounting & Administration Manager, Human Resources Manager, Import Manager;
- Commercial Director, Retail Managers, Real Estate Manager, Business Operation Control Manager;
- Product Director, Product Managers, Technical Services Manager, Sourcing Manager;
- Marketing Manager, Branch Merchandising & Administration Manager, IT Manager, Merchandising Manager, Logistic Manager.

11.3 THE SYSTEM IN GENERAL

All Sensitive Operations must be carried out in compliance with applicable legislation, the rules of the Code of Conduct, and the rules in this Model.

Generally, the Company's organization system must comply with the fundamental requisites of formality and clarity, disclosure and segregation of roles, especially with respect to the assignment of responsibilities, representation, definition of reporting lines, and operating activities.

The company must feature organization tools (organization charts, organization notices, procedures, etc.) inspired by the general principles of:

- Full disclosure within the Company;
- Clear and formal definition of roles, with a full description of the tasks of each function and related powers;
- Clear description of reporting lines.

Internal procedures feature the following elements:

- Segregation, within each process, between the person that starts it (decision-making), the person who performs it and completes its, the person who controls it;
- Written record of each significant step of the process;
- Appropriate level of formalization;
- Preventing bonus systems dedicated to roles with disbursement powers or with externally-relevant decision-making authority from being based on performance targets that are basically unachievable.

11.4 THE SYSTEM OF THE DELEGATION OF POWERS AND POWERS OF ATTORNEY

In principle, the system of delegation of powers and powers of attorney must feature elements of "certainty" for the purpose of preventing Offenses (traceability and records of Sensitive Operations) and, at the same time, allow the efficient management of business operations.

"Delegation of powers" means an action internal to the Company whereby functions and tasks are assigned, which is reflected in the system of organization notices.

"Power of attorney" means the unilateral legal instrument whereby the Company grants powers to represent it before third parties.

Holders of a corporate function who, to perform their tasks, need powers to represent the Company are granted a "general functional power of attorney" whose scope is appropriate and consistent with the functions and operating powers granted to the holder by way of a "delegation of powers".

The essential requisites of the system for the delegation of powers, with a view to an effective prevention of Offenses, are:

- All those (including Employees or Corporate Bodies of Service Companies) that maintain relations with GA on behalf of the Company must be appointed to such effect, pursuant to the Procedure for relations with GA.

The essential requisites of the system for granting of powers of attorney, with a view to an effective prevention of Offenses, are:

- General functional powers of attorney are granted only to persons with an internal delegation of powers or with a specific engagement agreement, in the event of stable service providers, which describes the relevant management powers and, where necessary, PoAs are accompanied by a specific notice which sets the scope of the powers of representation and possibly disbursement caps, referring in any event to compliance with the restrictions set by Budget approval processes and extra budgets, if any, and by Sensitive Operations monitoring processes by different functions;
- powers of attorney may be granted to individuals that are expressly identified in the instrument or to legal entities that will act through their attorneys that are vested, in the PoA, with similar powers.

The SC, with the support of other responsible functions, periodically audits the system of delegations of powers and powers of attorney in force and their consistency with all the system or organization notices (meaning documents internal to the company whereby powers are delegated), recommending any changes where management powers and/or the title fail to match the powers of representation granted to the attorney, or in the event of other discrepancies.

11.5 GENERAL PRINCIPLES OF CONDUCT

The following general prohibitions apply both to Employees and Corporate Bodies of the Company – directly – and to Service Companies, Consultants and Partners pursuant to specific contract clauses.

Performing, cooperating or causing the perpetration of conducts which, if taken individually or collectively, qualify directly or indirectly as the offenses included in the ones referred to above (art. 24 and art. 25 of Leg. Dec. 231/2001) is prohibited, as are any breaches of the corporate principles and procedures described in this Special Section.

In connection with such conducts, (consistently with the principles of the Code of Conduct) it is expressly prohibited to:

- Give or promise to give cash to Italian or foreign public officials;
- Distribute complimentary gifts and presents other than in compliance with corporate practice (i.e., any form of present offered in excess of standard business or courtesy practices, or howsoever aimed at acquiring a favorable

treatment in any Company business). Specifically, any present to Italian and foreign public officials or their family members is prohibited (including in countries where making gifts is a frequent practice) if this is capable of influencing independent judgment or lead to ensure any advantage for the Company. Allowed gifts are always of petty value or are aimed at promoting charity or cultural projects, or the trademark. Presents – except for the ones of petty value – must be recorded appropriately to enable audits by the SC;

- Grant advantages of any nature (promises of employment, etc.) to any representatives of Italian or foreign Government Agencies capable of having the same consequences as the ones described in the previous item;
- Render services to the benefit of Service Companies, Consultants and Partners that are not appropriately justified by the contractual relation in progress with them;
- Give remuneration to the benefit of Service Companies, Consultants and Partners that is not appropriately justified by the type of engagement to perform and locally applicable practice;
- Submit misrepresentations to national or EC government entities to obtain government funding, contributions or subsidized loans;
- Allocate amounts received from national or EC government entities as government funding, contributions or subsidized loans for purposes other than the ones to which they were destined.

Specifically, pursuant to the policy on the management of sponsorships, complimentary gifts and donations, members of Government Agencies or their family members must not directly or indirectly be offered or promised of any form of gift or free services capable of appearing, howsoever, connected with the business relation with the Company or aimed at influencing their independent judgement or cause to secure any advantage.

In cases where it is common practice in the environment in which a company operates to make presents and gifts/sponsorships, the offering party must timely inform his immediate superior who will submit the report to the SC. In any event, in case of gifts consisting in stocks on inventory, the offering corporate division sends a specific authorization request to the Retail Managers with the accurate indication of the product codes being given. The present may be given only if the Retail Managers approve.

Contributions and funding for political and welfare purposes must remain within the caps admitted by the law and be approved beforehand by the Board of Directors or by the corporate functions designated to such effect. It is also prohibited to submit misrepresentations to national or EC government entities to obtain government funding, contributions or subsidized loans, and to allocate any amounts received from national or EC government bodies as funding, contributions or subsidized loans to purposes other than the ones to which they were destined.

11.6 SPECIFIC PROCEDURAL PRINCIPLES

In liaising with Government Agencies, all Addressees of the Model are required to comply with the following rules of conduct:

a. Relations with Government Agencies must be inspired by full disclosure, cooperation, availability and full respect of their role and applicable laws and regulations, rules of conduct stated in the Code of Ethics and this Special Section, with accurate and prompt performance of its requirements and obligations;

b. Relations with Government Agencies must be handled solely by appropriately authorized parties based on the existing system of powers;

c. In case of exceptional events or critical circumstances that cannot be solved in the course of day-to-day relations with Government Agencies, staff must immediately report the situation to their immediate superior for any appropriate action;

d. Staff must not follow through with and is required to immediately report to their immediate superior any attempt at bribery or extortion by any official of Government Agencies which they are addressed or simply acquired knowledge of;

e. in case of inspections by public officials or entities entrusted with the provision of a public service, these relations must be with the presence of at least two parties, the Manager of the Relevant Division/Department and a human resource designated by the latter to manage relations with Public Officials.

   The Relevant Department/Division Manager is responsible for keeping record of the requests it receives, of minutes prepared by public officials in the event of inspections, and any information, data and documents delivered, made available and/or disclosed.

f. Any information that may be collected while performing one's tasks, regardless of the position, is always "*privileged and confidential*". This information must not be disclosed to third parties (including any persons directly or indirectly connected with Government Agencies) to obtain any form of potential advantage;

g. Recruiting staff or independent contractors must follow the rules of assessment of professional skills and total remuneration must be in line with what is already set for positions with similar functions and responsibilities, preventing any advantage to persons that could, directly or indirectly, carry out activities or play roles connected to Government Agencies;

h. The selection of suppliers must be based on several quotations by different parties, comparable among them in consideration of the type of products/services, assessing the best price and quality ratio.

   The rules to select suppliers must comply with the Code of Ethics to prevent the risk that the choice of the supplier is based on influences or is made to secure advantages by selecting suppliers with connections with Government Agencies, with the risk of perpetrating bribery and extortion;

i. Addressees must not attempt to influence the judgment of any civil servant or representative of Government Agencies, or any party connected thereto, by promising or giving cash, gifts or loans, or other illegal incentives. To ensure compliance with these rules, all gifts howsoever regarded in line with the foregoing must be agreed on beforehand with the immediate superior. Documents submitted while managing gifts must be duly kept to ensure traceability of any adopted action;

j. If the Company were to resort to contributions or loans granted by Government Agencies to organize training or education classes for Employees, the persons in charge of preparing documents supporting participation in the call must ensure that information is accurate and complete to prevent delivering misrepresentations or misleading information. Persons responsible for the management and use of resources must ensure that such resources are used in compliance with assigned destinations. Those who have controlling and supervising functions on accomplishments connected with the above operations (invoice settlement, destination of funds obtained from the State or EC bodies, etc.) must be very careful in performing accomplishments and immediately report to the SC any irregularity or discrepancy;

k. Notices and payments to mandatory insurance bodies based on contributions must be true and accurate, since any omission or alteration of data would trigger an attempt to fraud Government Agencies;

l. Notices and payments to social security and welfare institutions (i.e. INPS, INAIL, personal additional welfare) must be true and accurate, since any omission or alteration of data would trigger an attempt to fraud Government Agencies;

m. Employees, Corporate Bodies, Service Companies, Consultants and Partners that materially liaise with GA on behalf of the Company must be officially granted authority to such effect (by specific delegation of powers to Employees and Corporate Bodies or in the relevant service or consulting or partnership agreement, in the case of the other parties). Where necessary, the above listed parties will be granted specific written power of attorney pursuant to all the criteria listed in § 11.4 above;

n. Any critical issue or conflict of interest which may arise in relations with GA must be reported to the SC in writing;

o. All terms and conditions of agreements between the Company and Service Companies, Consultants and Partners must be in writing and such agreements must be proposed or verified or approved by the Company and comply with the following paragraphs;

p. Agreements with Service Companies, Consultants and Partners must contain standard clauses, defined by mutual agreement by the SC and external lawyers, on compliance with Leg. Dec. 231/2001;

q. Consultants and Partners must be selected with clear methods and following a specific procedure;

r. Agreements with Service Companies, Consultants and Partners must contain a specific statement by these parties that they are aware of the provisions in Leg. Dec. 231/2001 and its impact for the Company, that they were never involved in legal proceedings for offenses contemplated in the Decree (or if they were, they must declare it with a view to greater attention paid by the Company if a consultancy or partnership agreement is entered into), that they undertake to comply with Leg. Dec. 231/2001[10];

s. Agreements with Service Companies, Consultants and Partners must contain a specific clause governing the consequences of breaches by such parties of the provisions in Leg. Dec. 231/2001 (e.g. termination clauses, penalties)[11];

t. No payment may be made in cash[12];

u. Expressly authorized persons must take part in legal, tax and administrative inspections (e.g. related to Leg. Dec. 81/08, tax and INPS inspections, etc.). The entire process concerning the inspection must be recorded in specific minutes, which need to be filed with the Company's records. If the closing report discloses critical issues, the SC must be informed in writing by the manager of the involved function[13;]

v. Those who should be possibly called to carry out "technical/political lobbying" with Italian and foreign government entities to safeguard the interests of the Company must inform the CEO at least every six months with a report on any significant projects in progress, their status, and upcoming steps which will be pursued. The CEO has to report annually to the Board of Directors and, with a written report, to the SC, any "technical/political lobbying" activities carried out by him and by other relevant functions.

[10] Pursuant to the "Disciplinary system and penalty mechanisms".
[11] Pursuant to the "Disciplinary system and penalty mechanisms".
[12] Pursuant to the "Policy for the management of financial resources".
[13] Pursuant to the "Policy for the management of relations with GA".

Addressees must also abide by the following rules of conduct in in managing accomplishments with Government Agencies:

a. Accomplishments with Government Agencies and preparation of the relevant documents must be performed in compliance with applicable laws and regulations and with the rules of conduct of the Code of Ethics and this Special Section;

b. Accomplishments with Government Agencies must be completed with the utmost diligence and professionalism so as to provide clear, accurate, full and true information avoiding, and in any case reporting to the SC, conflict of interest situations. Documents must be processed timely accurately and in clear, objective and exhaustive language;

c. All documents must be verified and signed by the person responsible to such effect;

d. Each company function is responsible for filing and keeping record of all the documents generated in (its) operations, as regulated in this rule of conduct, including documents sent to Government Agencies electronically. These documents include, but are not limited to:

   d.1 licenses, authorizations and similar documents connected to the Company's business or obtained for other purposes, and agreements with contract parties that are public officials or government entities/entities entrusted with the provision of a public service;

   d.2 instruments, minutes, financial statements, forms, statements concerning the management of legal, tax and corporate affairs of the Company or administrative, social security and welfare issues related to staff;

   d.3 minutes of inspections, investigations and similar proceedings;

   d.4 documents for civil litigation, criminal proceedings, tax and administrative litigation, etc.;

e. Where accomplishments are completed using the IT system of Government Agencies, the Company prohibits any alteration to such system or the data stored in it;

f. In addition to complying with the principles and rules in the Model, all Employees and Partners that have relations with Government Agencies

are required to sign, upon request, a description of any sensitive transactions that they completed.

11.7 SPECIAL PROCEDURAL PRINCIPLES IN THE EVENT OF SPECIFIC RISK-FEATURING TRANSACTIONS

Due disclosure must be given in the event of transactions related to participation in procedures such as obtaining grants, contributions or subsidized loans by Italian or foreign government entities, transactions involving agreements and/or licenses with government entities or the issue of new licenses, or authorizations and permits, since in this Model these transactions are regarded as Risk-Featuring Transactions.

To such effect, the CEO or a Function Manager designated by the latter must appoint in writing an "internal manager" responsible for the individual Sensitive Transaction referred to above, except in case of the existence if an appropriate power of attorney or equivalent document. Generally, this is the person that manages such transaction and is the contact person.

The person in charge of managing the transaction reports the event to the SC through the dedicated information flow, whose contents, timing, and manners are extensively described in the relevant procedure that regulates sensitive activities.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION B
Corporate Crime

12. CORPORATE CRIME

12.1 CASES OF CORPORATE CRIME (ART. 25 TER OF DEC. LEG. /2001)

This Special Section refers to corporate crime.

Contemplated offenses are described in art. 25-ter of Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

12.2 SENSITIVE PROCESSES IN CONNECTION WITH CORPORATE CRIME

The following sensitive processes emerged in connection with corporate crime as per letters from a) to s) of paragraph I of art. 25 ter:

- Bookkeeping and managing operations related to the process to prepare the annual accounts and interim financial statements with reference to preparing data for corporate reporting or financial statements, measuring, recording and representing the Company's operations in accounting records, financial statements, reports and other corporate documents with respect to the risk of:
  - Material alteration of accounting data;
  - Artful estimates of assets or property of the Company;
  - Falsa recognition, recording and representation of accounting records;
  - False recognition, recording and representation of annual accounts and periodic reports;
- Treasury management;
- Preparing reports to shareholders and/or third parties on the Company's assets and liabilities, revenues and charges, and cash flows;
- Managing relations with shareholders, audit companies, Board of Statutory Auditors, with reference to the risks of:
  - Concealing documents or interfering with operations;
  - Carrying out activities that affect the control action of the audit company;
  - False corporate reports to the shareholders, false material facts subject of valuations;
  - Preparing false data for corporate reporting or for financial statements;
  - False recognition, recording and representation of business operations in accounting records, financial statements, reports and other corporate documents;

  - False representation, drafting of documents or reporta to Supervisory Authorities;
  - Material alteration of accounting data;
  - Artful estimates of assets or property of the Company;
  - Refunding, including simulated refunding, of contributions to shareholders or releasing the latter from the obligation of completing any fully or partially incomplete contribution;
  - False recognition, recording and representation of the annual report an six-month report;
  - Failure to report conflicts of interest;
- Relations with supervisory authorities (including but not limited to: Revenue Agency, Customs Agency, Tax Police, etc.);
- Transactions involving the capital and allocation of profits with reference to:
  - Capital reduction operations;
  - Returning contributions to shareholders or releasing them from the obligation of completing any fully or partially incomplete contribution;
  - Estimating assets or property of the Company;
  - Mergers, demergers or contributions where creditors or the Court object to such transaction;
  - Failure to report conflicts of interest;

  and the risks of:
  - Allocation of profits/advances on profits that have not actually been achieved;
  - Distribution of reserves, including reserves that were not formed with profits, which cannot be distributed by law;
  - Allocation of shares in the Company against considerations that are lower than face value;
  - Mutual subscription of shares;
  - Material overstatement of contributions in kind or receivables or the Company's equity, in the event of conversion;
  - Purchase or subscription of shares in related companies;
- Disclosing, holding and recording shareholders' meetings.

In addition, the following sensitive processes emerged in connection with private-to-private corruption in letter s-bis) of paragraph I of art. 25 *ter*:

- Managing relations with the audit company;
- Managing contracts / framework agreements;
- Managing works contracts and service agreements;
- Receivables cycle – sales to private individuals / Sales of goods, raw materials and services;
- Managing consulting services;
- HR Selection and recruiting;
- Managing insurance services.

Involved Company Roles:

- CEO;
- CFO, Treasury Manager, Financial Control, Accounting & Administration Manager, Human Resources Manager, Import Manager, Financial Control Manager;
- Commercial Director, Retail Managers, Real Estate Manager, Business Operation Control Manager;
- Product Director, Product Managers, Technical Services Manager, Sourcing Manager;
- Marketing Manager, Branch Merchandising & Administration Manager, IT Manager, Merchandising Manager, Logistic Manager.

12.3 GENERAL PRINCIPLES OF CONDUCT

This Special Section expressly prohibits Corporate Bodies (and Employees and Consultants to the extent necessary for the functions they perform) to adopt, cooperate or cause the adoption of conducts which, taken individually or collectively, directly or indirectly qualify as the offenses included in the ones referred to above (art. 25 *ter* of Leg. Dec. 231/2001).

Breaches of the principles and policies in this Special Section and of the operating procedure to manage reporting and closing of accounts are also prohibited.

It is expressly prohibited to:

a. Give misleading information on the Company's assets and liabilities, revenues and charges, and cash flow; specifically, the Company in connection with the process of closing year-end and mid-year accounting

statements, must be inspired by the principles of full disclosure and complete accounting information, and clear, accurate and true reporting;

b. Carry out actions aimed to harm the interests of shareholders and creditors through fraudulent and targeted actions;

c. Perform simulated transactions or disseminate information on non-listed financial instruments to cause a noticeable alteration in the price of such instruments;

d. Carry out procrastinating or obstructive action to hamper, slow down or mislead the supervisory and control operations performed by Supervisory Authorities, trade unions and audit companies.

With reference to the offenses in letters from a) to s) of paragraph I of art. 25 *ter,* this Special Section accordingly sets out the express obligation for the parties listed above to:

- Comply with accounting principles of reference;
- Ensure that all transactions are not only correctly booked, but also authorized, verifiable, lawful, consistent and appropriate;
- In recording the Company's operations in the accounting records and in preparing Financial Statements, adopt a fair, transparent and cooperative conduct;
- Prepare the relevant documents with the utmost diligence and professionalism so as to provide clear, accurate, complete and true information, preventing, and in any event reporting, in appropriate forms and manner, any conflict of interest situation;
- Proceed with the valuation and recording of assets and liabilities or revenues and charges in compliance with the prudent and reasonable basis of accounting, showing clearly, in relevant documents, which principles led to the determination of the value of the element;
- Pay careful attention when estimating accounting items: parties involved in the estimate process must comply with the reasonable basis of accounting and clearly describe valuation parameters followed, giving all additional information as necessary to ensure accuracy of the document;
- Make the draft annual financial statements and other accounting documents available to Directors and other corporate bodies duly in advance on the meeting for the approval of the draft financial statements and other accounting documents;
- Reply timely and fully to any request for documents by the Board of Statutory Auditors and by the party in charge of the audit of accounts, in the course of audit operations;
- Strictly comply with all laws and regulations protecting the integrity and effectiveness of the corporate capital, with reference to capital increase, the

allocation of profits and reserve, the distribution of interim dividends, to avoid any adverse effect on the guarantees of creditors and third parties in general;
- Guarantee that shareholders' meetings and relations with shareholders are in compliance with the provisions of the law and the bylaws;
- Ensure the regular operation of the Company and the Corporate Bodies, guaranteeing and favoring any form of internal control on corporate operations under the law, and the free and fair formation of the intentions of the shareholders' meeting;
- Adopt a fair, transparent and cooperative conduct with Corporate Bodies, with a view to enabling them to carry out the tasks assigned to them;
- Ensure that all extraordinary transaction are not only recorded in compliance with the law, but also legitimate, authorized and verifiable;
- Ensure the constant alignment between user profiles assigned and their roles within the Company, guaranteeing compliance with the rules on the segregation of duties between the person that perform the transaction, the person that records it in accounting and the persons that audits it;
- Ensure full traceability of the decision-making and authorization processes, and of completed audit activities, filing all supporting documents in a correct and detailed manner.

In connection with these conducts, it is expressly prohibited to:
- Represent or transmit for processing and representation in financial statements, reports and schedules or other corporate disclosures, any false or incomplete data or data that is not consistent with facts, with the statement of assets and liabilities, with the income statement or the cash flow statement of the Company;
- Omit data and information required by the law on the Company's assets and liabilities, revenues and charges and cash flow statement;
- Carry out any action aimed at giving misleading information with reference to the actual situation of the Company, failing to provide a fair representation of the Company's assets and liabilities, revenues and charges and cash flows;
- Carry out activities and/or transactions aimed at creating off-accounts cash (for instance by using invoices issued by third parties for inexistent transactions), or aimed to create "slush funds" or "parallel accounting", including for values that are below the thresholds of punishment under arts. 2621 and 2622 of the Italian Civil Code;
- Alter or destroy documents and financial and accounting documentation available online through unauthorized accesses or other actions to such effect;

- Return contributions to shareholders or release them from the obligation to perform them, except for the cases of lawful reduction of the corporate capital;
- Allocate profits or interim profits that were not actually earned or which the law requires to be allocated to reserve, or distribute reserves, including reserves other than profit reserves, which cannot be distributed by law;
- Purchase or subscribe to shares outside the cases admitted by law, with an adverse effect on the integrity of the corporate capital;
- Implement reductions of the corporate capital, mergers or demergers, in breach of the law on the protection of creditors, causing damages to them;
- Proceeding with fictitious formation or increase of capital, allotting shares for a value that is lower than their face value upon increasing the capital;
- Determine majorities in shareholders' meeting with fraudulent or simulated actions;
- Set up relations or carry out extraordinary deals with potential target when there is a reasonable suspicion that it may expose the Company to the risk of committing (including as accomplice) criminal conspiracy, terrorism financing, or money laundering, handling or using cash, assets or other benefits with an unlawful origin;
- Adopt conducts that materially prevent, by concealing documents or using other fraudulent means, or howsoever prevent control and audit activities on Company operations by the Board of Statutory Auditors or the audit company;
- Conceal or destroy correspondence or any other documents concerning the activities listed in this Special Section.

This Special Section sets out, with reference to the offense in letter s-bis) of para. I of art. 25 *ter*, the express obligation for Corporate Bodies (and Employees and Consultants to the extent necessary for the functions they perform) to:

- Distribute complimentary gifts and presents in excess of company policy (meaning any form of gift in excess of standard commercial or courtesy practices, or howsoever aimed at acquiring preferential treatment in any business of the company). Specifically, any form of gift to Italian and foreign parties or their family members (including in countries where making gifts is common practice) that may influence their independent judgement or lead to securing any advantage for the business. Admitted complimentary gifts are always of petty value or aimed at promoting charitable or cultural activities, or the brand. Gifts made – except for the ones of petty value – must be appropriately recorded to allow audits by the SC;
- Grant advantages of any nature (cash, promises of employment, etc.) to the benefit of representatives of companies, entities or businesses that may determine the same consequences as are described in the previous paragraph;

- Render services to the benefit of Service Companies, Consultants and Partners that are not appropriately justified by the contractual relation in progress with them;
- Pay remuneration to the benefit of Service Companies, Consultants and Partners that are not appropriately justified by the type of engagement to carry out and locally applied practice;
- Refrain from starting, in the course of business negotiations, requests or relations with a private party, the following actions (directly or indirectly):
  - Examine or offer employment and/or business opportunities capable of being an advantage to employees of private parties;
  - Request or obtain confidential information capable of jeopardizing the integrity or reputation of both parties.

12.4 SPECIFIC PROCEDURAL PRINCIPLES

All Addressees of Conbipel's Model are required to follow the following rules of conduct:

a. Reports to (Italian, supranational or foreign) Supervisory and Control Authorities or Bodies, including corporate bodies, of the market or of shareholders required by laws and regulations must be sent correctly and in due time, in a true and complete manner;

b. full and immediate cooperation must be given to Supervisory and Control Authorities or Bodies, providing timely all requested documents and information;

c. accounting standards must be complied with and, in the presence of any adjustments to them, where unreasonable, these must be immediately reported to the Surveillance Committee;

d. the rules of segregation of duties between who completes the transaction, who records it in accounts, and who audits it must be ensured;

e. staff cannot follow up and must immediately report to their manager any attempted bribery or extortion by any official of Government Agencies which they were involved in or simply acquired knowledge of;

f. in the event of inspections by Supervisory Government Authorities, the Addressees of this Special Section must handle such relations in the presence of at least two persons, where possible;

g. in the event of extraordinary transactions on the Company, Addressees of this Special Section must allocate profits, in full or in part, solely where such profits have actually been achieved;

h. purchase or subscription to shares of the Company must be in compliance with applicable legislation;

i. no dissemination of false information, no simulated transactions or other conduct with a fraudulent nature concerning non-listed financial instruments to generate a noticeable price alteration.

Preparing reports to shareholders and/or third parties on the Company's assets and liabilities, revenues and charges, and cash flows (annual financial statements, quarterly and six-month reports).

Annual financial statements must be prepared based on specific applicable company procedures which[14]:

- clearly determine data and information that each function is required to give, through their managers, for required reporting, criteria for processing data to be supplied, and timing of data delivery by each involved function to responsible functions;
- establish the transmission of data and information to the responsible function through an (IT) system which allows to trace single steps and to identify who enters data in the system.

To supplement existing procedures, the following additional requirements must be implemented:

- establishment of a procedure that includes at least one meeting between the CEO or the CFO, the audit company and the Board of Statutory Auditors. This meeting must be held before the Board of Directors' meeting called to approve the draft annual financial statements and serves the purpose to review and assess the draft financial statements to determine if the information in them is accurate and complete;
- the draft financial statements and the auditor's and the Board of Statutory Auditors' reports to such financial statements must be made available to all members of the Board of Directors without delay, and appropriate documentation of delivery of such documents must be prepared and filed with the company's records.

Managing relations with the Board of Statutory Auditors

In relations with the Board of Statutory Auditors, the following requirements are adopted:

- the members of the Board of Statutory Auditors, identified in para. 2 of art. 2397 of the Italian Civil Code, must be chosen according to applicable legislation (they must be registered in professional rolls with the relevant professional association or bars, monitored by the Ministry of Justice, such as university professors, lawyers, certified public accountants, payroll

[14] According to the Procedure "Managing reporting & financial statements closing activities".

consultants). Any person that is in the conditions referred to in art. 2382 and art. 2359 of the Italian Civil Code cannot be appointed as statutory auditor and if elected automatically forfeits office. Statutory Auditors are responsible for performing their functions and duties with the professionalism and diligence required by the nature of their office, according to art. 2407 of the Italian Civil Code. The action for liability against statutory auditors is governed by art. 2393 and art. 2394 of the Italian Civil Code. Statutory Auditors are required to carry out their duties with the diligence of the appointed offices under art. 1710 of the Italian Civil Code, they are responsible for the truth of their statements and are required to treat as confidential any facts and documents that they acquire knowledge of because of their office, as required by art. 2622 of the Italian Civil Code, read in conjunction with art. 622 of the Italian Criminal Code.

Managing relations with the independent audit company

In relations with the independent audit company, the following requirements are adopted:

- compliance with the procedure that regulates the steps to assess and select the audit company;
- consultancy engagements, for services other than the audit of accounts, may be granted to the audit company or to companies or professional entities belonging to the same group as the audit company, only if authorized by the CEO.

Other rules aimed at preventing corporate crimes in general with reference to the offenses in letters from a) to s) of para. I of art. 25 ter.

In addition to the rules of the organization structure and existing procedures, the following additional requirements are implemented:

- implementing a periodic training-knowledge plan for significant staff on the rules of the organization structure and on corporate crime;
- scheduling periodic meetings between the Board of Statutory Auditors and the SC to determine compliance with provisions of corporate regulations;
- transmitting to the Board of Statutory Auditors, duly in advance, all documents concerning items on the agenda of shareholders' meetings or meetings of the Board of Directors or items on which it is required to give an opinion pursuant to the law;
- formalization and/or revision of internal regulations and procedures concerning compliance with the law.

With reference to the offense in letter s-bis) of para. I of art. 25 ter, the procedures described below must be followed, in additions to the General Rules and Principles of this Model. The following rules must be complied with when carrying out one's duties in Italy and abroad.

- Employees, Corporate Bodies Service Companies, Consultants and Partners that materially take part in managing sensitive processes in connection with the offense of private-to-private corruption and incitement to private-to-private corruption on behalf of the Company must be officially granted powers to such effect (with a specific delegation of powers in case of Employees and Corporate Bodies, or in the relevant service or consultancy or partnership agreement in case of the other parties). Where needed, such parties will receive a specific written power of attorney;
- Agreements between the Company and Service Companies, Consultants and Partners must be entered into in writing with respect to all terms and conditions, and proposed or checked or approved by at least two people belonging to the Company, and comply with the following paragraphs;
- HR selection and management is governed by a specific policy[15];
- Management of consulting services is governed by a specific policy[16];
- Agreements with Service Companies, Consultants and Partners must contain standard clauses, defined in agreement by the SC and external lawyers, with a view to compliance with Leg. Dec. 231/2001;
- Consultants and Partners must be selected with transparent methods and according to a specific policy[17];
- Agreements with Service Companies, Consultants and Partners must contain their express statement that they know the provisions in Leg. Dec. 231/2001 and its implications for the Company, that they were never involved in legal proceedings for offenses contemplated in such Decree (or if they were, they must declare it for the purposes of greater attention by the Company in case a consultancy or partnership agreement is entered into), that they undertake to comply with Leg. Dec. 231/2001[18];
- Agreements with Service Companies, Consultants and Partners must contain a specific clause regulating the consequences of their breaches of the provisions in Leg. Dec. 231/2001 (e.g., express termination clauses, penalties) [19];
- The Addressees of the Model comply with the "Preventing Private-to-Private Corruption" policy.

[15] "HR Management" Policy.

[16] "Purchase of goods and services that are not related to products" policy and "Management of purchase of goods and services related to products".

[17] "Purchase of goods and services that are not related to products" policy and "Management of purchase of goods and services related to products".

[18] Pursuant to the "Disciplinary and penalty system".

[19] Pursuant to the "Disciplinary and penalty system".

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION C AND SPECIAL SECTION C-BIS

Receiving, laundering and using cash, assets or benefits of a criminal origin, and self-laundering and Crimes for the purposes of terrorism or subversion of the democratic order

13. RECEIVING, LAUNDERING AND USING CASH, ASSETS OR BENEFITS OF A CRIMINAL ORIGIN, AND SELF-LAUNDERING, AND CRIMES FOR THE PURPOSES OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER

This Special Section concerns the offenses of receiving, laundering and using cash, assets or benefits of unlawful origin and self-laundering as well as crimes for the purposes of terrorism or subversion of the democratic order.

Individual crimes addressed are the ones in art. 25-octies and 25-quater of Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

Predicate offenses of self-laundering under art 648-ter.1 of the Criminal Code are all offenses committed with willful intent that generate proceeds capable of being the subject of economic evaluation – basically any form of crime capable of generating proceeds – and these may concern not only illegal cash flows originated outside the Company, but also cash, assets or other benefits already included in the Company's assets, that are later used in entrepreneurial, business, financial operations of the entity, thus creating an actual obstacle to the identification of the criminal origin of such resources. Accordingly, self-laundering will be dealt with in a specific section: SPECIAL SECTION C-BIS.

13.1 SPECIAL SECTION C: RECEIVING, LAUNDERING AND USING CASH, ASSETS AND BENEFITS OF UNLAWFUL ORIGIN (ART. 25 OCTIES OF LEG. DEC. 231/2001) AND CRIMES WITH THE PURPOSE OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER (ART. 25 QUATER LEG. DEC. 231/2001)

The following sensitive processes emerged in connection with receiving, laundering and using cash, assets or other benefits of unlawful origin (art. 25 octies of Leg. Dec. 231/2001, except for self-laundering - art 648-ter.1 of the Criminal Code – and crimes with the purpose of terrorism or subversion of the democratic order (art. 25 quater of Leg. Dec. 231/2001):

a) Relations with third parties for:
   - Purchase and/or sale agreements with other parties;
   - Financial transactions with other parties;
   - Investments with other parties;
   - Sponsorship activities.

13.1.1 SENSITIVE PROCESSES IN CONNECTION WITH RECEIVING, LAUNDERING AND USING ILLEGAL BENEFITS AND WITH CRIMES WITH THE PURPOSE OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER

CONBIPEL S.p.A. does not fall within the scope of applications of the provisions of Leg. Dec. 231/2007, because it is not a financial intermediary and it does not belong to the category of other players referred to in art. 14 of such legislative decree.

Accordingly, it is not required by the law to identify customers, record and report suspicious transactions as per the legislation referred to above. Nonetheless, the current organization system of the company features the presence of multiple tools aimed to prevent the offenses of receiving, laundering or using cash assets or benefits of unlawful origin.

With reference to the other offenses under art. 25 *octies,* the following sensitive processes are regarded as featuring risks:

- Treasury management (payments received and made) including by bearer securities;
- Procurement of goods and services and granting professional and consultancy engagements;
- Managing sales to stockists;
- Investment management;
- Managing extraordinary and intercompany transactions;
- Managing Employees' and Consultants' expense refunds;
- Loan management;
- Making donations and complimentary gifts;
- Managing relations and accomplishments with Government Agencies, and managing accounting records and financial statements, with specific reference to calculating, booking and paying taxes.

While with specific reference to the offenses under art. 25 *quarter* the following sensitive processes are regarded as featuring risks*:*

- Purchase and sale of goods/services from/to risky parties;
- Investments with risky parties;
- Selecting business/financial patterns and managing relevant relations with risky parties.

<u>Involved Company Roles:</u>

- CEO;
- CFO, Treasury Manager, Financial Control, Accounting & Administration Manager, Human Resources Manager, Import Manager;
- Commercial Director, Retail Managers, Real Estate Manager, Business Operation Control Manager;
- Marketing Manager, Branch Merchandising & Administration Manager, Merchandising Manager, Logistic Manager.

13.1.2 GENERAL PRINCIPLES OF CONDUCT

The following general prohibitions apply directly to Corporate Bodies, executives and Employees, while they apply to Consultants, suppliers and Partners pursuant to specific contract clauses.

These parties must not adopt, take part in or cause the adoption of conducts which, taken individually or collectively, trigger directly or indirectly the above offenses. It is also prohibited to breach corporate principles and policies set out in this Special Section.

In accordance with the Code of Ethics, procedures, policies and corporate rules, the parties listed above must not by way of example:

- Make transfers of cash when the value of the transaction, including if split, is aggregately equal to or higher than €3.000,00 (the transfer may be made through banks, e-money and the Italian postal system, i.e. Poste Italiane S.r.l.);
- Issue bank and postal checks for amounts equal to or higher than €3.000,00 that do not have the indication of the name or company name of the beneficiary and the "non-transferable" clause;
- Endorse for collection bank and postal checks issued in the name of the drawer if this is not a bank or Poste Italiane S.r.l.;
- Transfer cash through payment service providers in the form of collection and transfer of funds;
- Make transfers of cash when there is no perfect match between payee/payor, payments and parties actually involved in transactions;
- open, howsoever, accounts or deposits anonymously or under a fictitious name and use any such accounts or deposits possibly opened in foreign countries;
- make international bank transfer that do not state the name of the other party;
- make bank transfers providing funds in cash to countries other than the one where the order originated.

The parties identified above must also follow the following general principles of conduct:

- refrain from adopting conducts capable of triggering money laundering;
- refrain from adopting conducts that, albeit alone do not trigger the above offenses, they could potentially become so;
- adopt a fair, transparent and cooperative conduct, in compliance with the laws and internal Company policies, in all operations aimed at managing lists of suppliers, customer and partners, including foreign ones;

- refrain from doing business with (natural or legal) persons that are known or suspected to belong to criminal organizations or in any case operating outside the scope of legality;
- constantly monitor corporate cash flows.

13.1.3 SPECIFIC PROCEDURAL PRINCIPLES

All Addressees of the Model involved in the sensitive process identified above must:

- Check the business and professional reliability of suppliers and business and financial Partners;
- Check that suppliers and Partners are not based or have their registered office or any connection with countries which the Financial Action Task Force on Money Laundering and Terrorist Financing (FATF) regards as uncooperative; if suppliers and Partners have any connection with one of such countries, relevant decisions must be expressly authorized by the CEO;
- Make formal and material checks on corporate cash inflows; such checks must consider the registered office of the other party (including, but not limited to, tax havens, countries with the risk of terrorism, etc.) and any sham companies and fiduciary schemes used for any extraordinary transactions.

In addition and to give operating details with respect to the principles outlined in the procedures referred to above and rules of conduct in the Code of Ethics, the corporate organization system features the presence of multiple tools aimed at preventing the offenses of receiving, laundering or using cash, assets or benefits of unlawful origin and crimes with the purpose of terrorism or subversion of the democratic order, and namely:

- procedures to select suppliers and store the relevant lists;
- procedures to manage payments received and recovery of receivables;
- procedures to manage payment-treasury;
- procedures to manage cash;
- financial resource management policy;
- expense reports and business trips policies;
- policy on the procurement of goods, services, consulting, professional services and intermediation;
- all policies on the management of relations with Government Agencies and Supervisory Authorities.

The above procedures require the identification and prior traceability of customers, except for private customers of stores, and suppliers, and the traceability of cash flows.

In light of the type of customers and suppliers of CONBIPEL, of the accomplishments which the Company is required to complete in connection with imports and exports, of the procedures which it adopted to comply with the statutory requirements under review, and the business system for the management of payments made and received, we are of the opinion that the risk of perpetrating the offenses of *receiving, laundering or using cash, assets or benefits of unlawful origin* and the risk of *crimes with the purpose of terrorism and subversion of the democratic order* is limited and in any event controlled through the procedures listed above.

13.2 SPECIAL SECTION C-BIS: SELF-LAUNDERING (ART. 25 OCTIES OF LEG. DEC. 231/2001)

Predicate offenses of self-laundering, art. 648-ter.1 of the Criminal Code, are all offenses committed with willful intent that generate proceeds capable of being subject of economic valuation – basically any form of crime capable of generating proceeds.

The new offense under review is committed if the following three conditions are met simultaneously:

i. One creates or participates in the creation of a funds consisting in cash, assets or other benefits is created by committing an initial offense, i.e., the predicate offense;

ii. Such funds are used in entrepreneurial, business and financial activities, through an additional separate action;

iii. A material obstacle is created in the identification of the criminal origin of such funds.

This led the Company to carefully assess the origin of amounts that become part of its assets, since legal persons are required to adopt important and effective systems to control the origin of such assets. The result was a separation of all potentially relevant operations into two categories:

a) Business operations where procedures and principles of conduct have already been adopted by the Company to prevent the risk of perpetration of predicate offenses under Leg. Dec. 231/2001, because cash, assets, or other benefit to be used to commit *self-laundering* could generate specifically from perpetration of such offenses, without prejudice to the need for all material and personal elements applicable to self-laundering to subsist;

   these types of sensitive activities / offenses include but are not limited to:

   - Certain offenses against Government Agencies such as “embezzlement”, “aggravated fraud to the detriment of government”, “improperly received contributions”, “bribery and extortion”;
   - A significant part of corporate crime, and namely "false corporate reporting", in its two major declinations of substantial forgery - alteration/adulteration of items in financial statements whose nature is certain – and intentionally false documents – alteration/adulteration of financial statements data whose nature is

estimated/assumed –more commonly known “false evaluation" and "private-to-private corruption ";

- Offenses against industry and trade, and primarily “fraud in exercising trade” and "trademark infringement";
- Environmental crimes, the most evident being “illegal waste trafficking”;
- Offenses in the area of copyright, specifically in connection with the “illegal reproduction and sale of works, products and/or databases owned by other parties”.

The offenses listed above are already included in the so-called catalog of predicate offenses under Leg. Dec. 231/2001 and accordingly the general principles of conduct and specific procedural principles will make reference to the specific Special Sections of the Model, to the principles of conducts, requirements and prevention policies already implemented to prevent such crimes;

b) Business operations that are relevant in connection with offenses that currently are not included in the catalog of predicate offenses under Leg. Dec. 231/2001. In connection with such operations attention needs to be paid to “**tax offenses**” that fall under crimes committed with willful intent whose proceeds are earned by the Company and almost automatically used in the business cycle. So, if a tax offense is committed in a business operation and in the interest of the Company, reusing the proceeds of the crime inside the Company is relevant for the purposes of self-laundering. For the offense to be triggered, however, an additional action to the conduct that resulted in the predicate offense must take place. That is a conduct aimed at materially preventing the identification of the unlawful origin.

With reference to these types of operations, sensitive processes which are considered as featuring risks are all the processes where conditions may occur to reuse, replace or transfer cash or other assets, such as:

- Income tax returns;
- Day-to-day tax accounting records;
- Investments;
- Audit of accounts;
- Intercompany transactions;
- FX Risk transactions.

Certain types of operations are not unrelated to the Model, but were already mapped in connection with sensitive processes related to corporate crime and creation of funds.

Specifically, relations with audit companies are analyzed in the paragraphs on corporate crime.

Certain processes were analyzed in connection with funds processes in connection with procurement of goods and services, management of consulting, recruitment and hiring of staff. Others were analyzed in connection with the offense of money-laundering, transnational crime and offenses in relations with Government Agencies.

13.2.1 GENERAL PRINCIPLES OF CONDUCT AND SPECIFIC PROCEDURAL PRINCIPLES

The following general prohibitions apply to Corporate Bodies, executives and Employees directly, while they apply to suppliers and Partners under specific contract clauses.

These parties are prohibited from adopting, participating in or causing the perpetration of conducts which, individually or collectively, trigger directly or indirectly the offenses falling in the category referred to above. Breaches of corporate principles and procedures in this Special Section are also prohibited.

Consistently with the Code of Ethics, corporate procedures, policies and regulations, prohibitions applicable to the parties identified above include but are not limited to:

The control system over the sensitive activities described above is based on the following qualifying elements guaranteeing objectivity and transparency of adopted choices, namely:

- Authorization levels are defined according to which decisions on investments may be taken only by bodies that have been expressly designated to such effect based on the existing system of powers and delegation of powers;
- Checks are made to determine that powers to authorize in the area of investment management are correctly and consistently applied;
- Segregation is applied in processes and this involve several players, with management, audit or approval responsibilities;
- The decision-making process is traceable thanks to the involved function documenting and filing all the documents concerning all the steps in the process.

General control principles therefore are:

- Prohibition to conceal proceeds from any offense committed purportedly in the interest or to the advantage of the Company;
- Guarantee of transparency and traceability of financial transactions;
- Using the banking system for transactions, where possible;
- Using only financial resources whose origin was determined and only for transactions that have an express reason and that are recorded in accounts and supported by documents;
- Formalization of terms and conditions in agreements that govern relations with suppliers and business and financial Partners, including companies of the same group;

that is, all elements capable of making “transparent” the purposes and the methods adopted for the transaction.

From a procedure point of view, all Addressees of the Model involved in the sensitive processes identified above are prohibited from:

- Altering, including partially, any supporting documentation of cost/outflow and revenue/inflow transactions;
- Generating and recording such documents in the absence of a payment and an economic agreement supporting and legitimating their issue;
- Fraudulently recording such documents in accounts converting administrative flows contained in them into accounting flows with a different information content – for instance, recording a taxable contingent asset in a capital reserve, without entries in the Company’s profit and loss account;
- Fraudulently recording such documents, booking in accounting records numbers and data that are different, by description and cause, from the ones stated in the relevant "supporting documents";
- Tampering with and/or fraudulently destroying such documents to prevent their entry in accounting records;
- misapplying/omitting to apply valuation rules and principles set out in articles 2423 and following of the Italian Civil Code on preparing the annual financial statements;
- filing annual VAT, income tax and withholding agent returns containing facts that are not true with willful intent;
- filing annual VAT, income tax and withholding tax agent returns omitting significant events and/or recordings of transactions that were recognized and/or included in the Company’s accounting records and contained in the annual financial statements, with willful intent;
- misapplying, when preparing the annual financial statements, accounting standards issued by the OIC (*Organismo Italiano di Contabilità*) for all the items that are not in fact regulated by the Italian Civil Code and in all cases in which legal principles concerning financial statements require an additional explanation/interpretation;
- committing, including as accomplice, any offense with willful intent (including tax offenses) that may generate cash, assets or other benefits capable of being replaced, transferred or used in business, financial or entrepreneurial or speculative operations.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION D

Manslaughter and serious and very serious unintentional injuries committed with breaches of accident-prevention provisions and occupational health, safety and hygiene legislation

14. MANSLAUGHTER AND SERIOUS AND VERY SERIOUS UNINTENTIONAL INJURIES COMMITTED WITH BREACHES OF ACCIDENT-PREVENTION PROVISIONS AND OCCUPATIONAL HEALTH, SAFETY AND HYGIENE LEGISLATION (ART. 25 SEPTIES OF LEG. DEC. 231/2001).

This Special Section concerns manslaughter and unintentional injuries committed with breaches of occupational health and safety laws and regulations, and specifically the offenses in art. 25 *septies* of Leg. Dec. 231/2001.

Accident-prevention and occupational health and safety regulations address specific persons and specifically the employer, executives, supervisors and workers. Certain specific provisions concern the manager of the prevention and protection service and the safety representative. With respect to temporary mobile works sites (for works in the new shops, maintenance of the central warehouse, etc.) a number of specific provisions involve the client, the works' manager and safety coordinators.

The purpose of this Special Section is that all Addressees, as identified above, adopt rules of conduct that are consistent herewith to prevent the occurrence of the offenses discussed in this Special Section.

Specifically, this Special Section intends to:

a) Give details on regulations that need to be complied with to correctly apply the Model;

b) Provide the SC and the managers of the other corporate functions that cooperate with it with implementation tools to exercise required control, monitoring and audit activities.

14.1 SENSITIVE PROCESSES RELATED TO MANSLAUGHTER AND UNINTENTIONAL SERIOUS OR VERY SERIOUS INJURIES COMMITTED WITH BREACHES OF ACCIDENT-PREVENTION PROVISIONS AND REGULATIONS ON THE PROTECTION OF OCCUPATIONAL HYGIENE AND HEALTH

Sensitive processes were identified in connection with business operations aimed to:

a) Set objectives that are in line with the business policy, define processes required to achieve objectives, determine and assign resources;

b) Define organization structures and responsibilities; training, consultation and communication methods; methods to manage the document system, to control documents and data; methods to control operations; emergency management;

c) Implement methods to measure and monitor performance, record and monitor accidents, non-compliances, corrective and preventive actions, methods to manage recording, periodic audit completion methods;

d) Carry out periodical reviews to assess if the occupational health and safety system is fully implemented and if it is sufficient to achieve the business policy and objectives.

Processes aimed to ensure a corporate system for the performance of all legal obligations concerning the issues listed below are regarded as sensitive processes:

- Compliance with legal technical-structural requisites concerning equipment, plants, systems, workplaces, chemical, physical and biological agents;
- Risk assessment operations and activities to set up consequent prevention and protection measures;
- Organization-related activities such as emergency and first aid, managing contracts for works and services, periodic safety meetings, consultation with workers' safety representatives;
- Health surveillance operations;
- Workers' knowledge and training activities;
- Supervisory activity with respect to compliance with safe work procedures and instructions by workers;
- Acquisition documents and certificates required by law;
- Periodic audits on the application and effectiveness of adopted procedures.

Major Sensitive Processes, that will have to be constantly monitored by the SC, are described below, it being understood that their regulation is also ensured by individual safety and health procedures and, more generally, by the internal control system, and accordingly through company regulations (rules, manual and automated procedures, manuals, operating instructions, policies, regulations, etc.) concerning all company systems (quality management system, management control and reporting system, administration, accounting and financial system, industrial and environmental safety management system, etc.), documents and provision on the hierarchical-functional and organizational structure of the company, the organized system of delegation of powers and powers of attorney.

14.2 GENERAL OVERVIEW

The Company prepared a corporate organization chart that defines roles based on a hierarchical structure regulated by a system of powers of attorney and delegations of powers.

Consistently with its organization structure, the Company identified the CEO as its Employer[20]. Appropriate powers were delegated in this respect.

The Company appointed the company physician[21] and designated the manager of the prevention and protection service[22] outside the Company.

The Company has the required accident logbook[23].

The Company completed the occupational health and safety risk assessment and prepared the relevant document, pursuant to the law[24].

The Company has the fire prevention certificate.

The Company complies with requirements on the protection of health and safety at workplaces, including by resorting to the contribution of external technical-professional consulting services.

To prevent more effectively the perpetration of the offenses in article 25-septies of Leg. Dec. 231/2001 – in its interest or to its benefit by the persons listed in article 5 of Leg. Dec. 231/2001, including acting as accomplice to other parties –, the Company has adopted and implemented specific health and safety procedures that were approved by the Employer and adapts its organization and operations to such procedures.

The Company ensure appropriate training and knowledge of directors and all subordinate Employees on the purposes and contents of the procedures.

[20] Historical report of the Chamber of Commerce.
[21] Instrument of appointment available at the Company.
[22] Instrument of appointment available at the Company.
[23] Available at the relevant Authority.
[24] Risk Assessment Document (DVR) in force available at the Company.

14.3 ORGANIZATION

14.3.1 IDENTIFICATION OF THE EMPLOYER

The Employers is identified in the CEO, to whom the Board of Directors granted exclusively any and all powers on occupational health and safety.

14.3.2 IDENTIFICATION OF EXECUTIVES AND SUPERVISORS AND, IN GENERAL, ASSIGNMENT OF DUTIES AND ROLES

The Employer, working with the manager of the protection and prevention service (hereinafter "RSPP") and the HR function, identifies "Executives" and "Supervisors", meaning the persons responsible for operations carried out in specific areas of the business.

Executives are duly empowered, by a power of attorney that includes the power to represent the Company in connection with occupational health and safety issued, in relation to the areas of the business assigned to them.

Organization notices[25] specify duties and responsibilities.

The same notices identify the criteria and the methods defined to assign tasks to workers.

Specifically, they define:

- criteria for granting duties to workers based on their skills, health and safety conditions, and the outcome of health checkups;
- organization measures for the Company Physician's and the RSPP's participation in the definition of workers' roles and responsibilities;
- traceability of assessment operations completed to such effect.

The appropriate and up-to-date natures of the identification of executives and supervisors are guaranteed by the RSPP's constant monitoring.

On a yearly basis, during the periodic meeting held pursuant to art. 35 Leg. Dec. 81/08, the RSPP reports on their monitoring and any consequent revisions.

14.3.3 DESIGNATING THE MANAGER OF THE INTERNAL OR EXTERNAL PREVENTION AND PREVENTION SERVICE, PURSUANT TO ART. 32 LEG. DEC. 81/08

The Employer designates the Manager of the Prevention and Protection Service, and any subsequent requirement, including with control agencies.

The designated person must have the requisites required by the law to carry out such assignment, proof of which needs to be given in designation notice letter.

[25] Organization notices "Safety organization and, delegation of powers and appointments" and "Functions' Roles and Responsibilities".

The notice referred to above must allow to trace checks completed on specific requisites required by applicable legislation, show that the assessment was completed to understand the manager's skills and available time to cover such role, and give proof of official acceptance of the assignment

The instrument of appointment must be filed by the RSPP, according to internal regulations governing document management roles and responsibilities in health and safety management[26].

14.3.4 APPOINTMENT OF THE COMPANY PHYSICIAN IN THE CASES SET OUT IN ART. 41 LEG. DEC. 81/08

The Employer appoints the Company Physician and performs any further requirement, including with control agencies.

The appointed person must meet the skills and requisites required by the law to carry out the assignment, which must be proved in the letter of notice on appointment.

This notice must allow to trace the checks completed on the specific requisites required by applicable legislation and official acceptance of the assignment.

The instrument of appointment must be filed by the RSPP, according to internal regulations governing roles and responsibilities in the management of occupational health and safety documents[27].

[26] "Document management" procedure.
[27] "Document management" procedure.

14.4 MONITORING – PERIODIC AUDITS – SURVEILLANCE

a) The employer and/or the holders of functions delegated by him and executives, with respect to their areas of responsibility, the RSPP and the company Physician perform the obligations to verify application and effectiveness, as required of them in the following paragraph LEGAL OBLIGATIONS and duly keep records of any relevant activity.

b) The employer and/or the holders of functions delegated by him plan and implement, in any case, appropriate periodic audits on compliance with legal occupational health and safety obligations and, upon their conclusion, adopt any necessary measure and keep records of any related activity.

c) Surveillance on policy implementation and on maintaining the appropriate nature of any adopted measures in time, the review and possible proposition of changes to the contents of the policy are made by the Surveillance Committee set up to such effect by the Company in compliance with the provisions on its appointment, duties and powers, operation, information flows and composition.

d) The review of and any amendment to the content of the policy are ordered whenever material breaches of regulations on accident prevention and protection and occupational health occur, or whenever changes occur to organization and operations further to scientific and technological progress.

14.5 LEGAL OBLIGATIONS

a) This Special Section relies on the assumption that the Company is actually aware of legal obligations applicable in the area of occupational health and safety.

b) To ensure appropriate knowledge, the RSPP sets up and maintains an updated file of applicable occupational health and safety regulations, highlights which ones are applicable to the Company and timely reports them to the employer and the holders of functions delegated by the latter, executives, company physician and to the workers' safety representative.

c) The RSPP processes and updates documents that set out, in the most simple, unambiguous, organized and exhaustive form, legal obligations on the protection of occupational health and safety for which the employer and the holders of functions delegated by the latter, executives, supervisors, the company physician, and the protection and prevention service are responsible.

d) The RSPP forwards to the employer and the holders of functions delegated by the latter, executives, supervisors, the company physician, and the protection and prevention service the documents stating legal obligations for which each role is accountable and any revision to such obligations.

e) The RSPP sets up and keeps an updated file of documents in item c) which were duly forwarded to the employer and the holders of functions delegated by the latter, executives, supervisors, the company physician and the prevention and protection service.

14.6 INVESTMENT PLAN AND ANNUAL BUDGED FOR ACTIONS IN THE AREA OF OCCUPATIONAL HEALTH AND SAFETY AND RELEVANT REPORTING

a) The employer and/or holders of functions delegated by the latter, working with the RSPP and, to the extent of their responsibilities, the company physician including on the basis on the applicable document "Environment and Safety Policy", define the yearly or multi-year plan for investments required to ensure that occupational health and safety levels are maintained and/or improved in time and also report, on an annual basis, on expenses disbursed and actions taken.

b) Yearly or multi-year plans clearly identify deadlines, responsibilities and availability of (financial, human, logistic, and equipment) resources necessary for implementation and must be disclosed to the organization so that staff may have a sufficient understanding.

c) The RSPP prepares a detailed report that is reviewed during the meeting referred to in art. 35 of Leg. Dec. 81/08 and is annexed to the relevant minutes along with the budget and accounting reports.

d) The employer and/or the holders of functions delegated by him ensure that the provisions of the investment plan are transposed in the corporate budget.

14.7 RISK ASSESSMENT – PREVENTION AND PROTECTION MEASURES

a) The employer, the RSPP and the company physician are required to comply with the obligations related to risk assessment and arranging consequent related prevention and protection measures as set out in § LEGAL OBLIGATIONS keeping records of any activity.

b) The RSPP appropriately checks that the persons required to do so performed activities aimed to assess risks, draft the relevant document, and possibly reprocess such risks.

c) The RSPP appropriately also checks that the employer and the company physician transmitted to the prevention and protection service all information on the nature of risks, work organization, planning and implementation of preventive and protective measures, description of production systems and processes, data on occupation accidents and professional diseases, and measure adopted by supervisory bodies.

d) The protection and prevention system constantly assesses, to the extent of its responsibility that prevention and protection measures are appropriate and effective on the basis of the control systems that it developed.

14.7.1 PREPARING AND REVISING THE RISK ASSESSMENT AND THE RISK ASSESSMENT DOCUMENT (DVR) UNDER ARTS. 28 AND 29 OF LEG. DEC. 81/08

a) The employers, with the support of the RSPP, drafts and maintains updated specific company regulations that identify roles, responsibilities and methods to carry out, approve and revise Corporate Risk Assessment. Company regulations must guarantee that the assessment:

- Identifies roles, authorities, skill requisites, and training needs of staff in charge of identifying dangers, identifying risks and controlling risks;
- Identifies responsibilities to check, approve and revise the contents of the el DVR;
- Identifies methods and criteria to revise in specific periods or timeframes danger identification and risk assessment process;
- Ensures, where necessary, mechanisms to trace the involvement of the company physician in the danger identification and risk assessment process;
- Sets out the assessment of the various type of sources of risks: standard or generic, ergonomic, specific, process and organization dangers, and identifies consistent areas in terms of danger inside the company;
- Identifies the representative duties of workers;

- Lists and describes the features of chemical agents and machines and equipment present in the company;
- Expressly defines assessment methods adopted for the different categories of risk in accordance with applicable regulations and requirements.

b) The Risk Assessment Document (DVR) is prepared based on Company regulations referred to in point a) and developed and revised according to the timeframes and methods required by the law by the Employer with the support of the RSPP and, to the extent of his responsibility, by the Company Physician. The process involves Supervisors and, in case of relevant elements, Engineers.

c) The DVR is constantly monitored by the RSPP that ensures its time revision.

d) The DVR must be available at the Prevention and Protection Service and, after each amendment and/or supplement, the RSPP must forward it to the workers' safety representative and the SC.

14.8 EQUIPMENT, SYSTEMS, WORKPLACES; CHEMICAL, PHYSICAL AND BIOLOGICAL AGENTS

a) The employer and the holders of functions delegated by him, executives, supervisors, the prevention and protection service and the company physician comply with obligations required of them in the paragraph § LEGAL OBLIGATIONS, and keep record of the relevant activities.

b) Compliance with statutory technical-structural standards on equipment, systems, workplaces, chemical, physical and biological agents is maintained by the employer or the holders of functions delegated by it by planning and implementing, with the support of the prevention and protection service and, to the extent of his responsibility, the company physicians, appropriate periodic audits performed by strictly referring to the contents of the risk assessment document and applicable laws and regulations.

c) Upon conclusion of the audits, the employer or the holders of functions delegated by him adopt any necessary measure to reinstate compliance with statutory standards.

d) In the event of any change to equipment, systems, workplaces, and to exposure to chemical, physical and biological agents, the employer and the holders of functions delegated by him, with the support of the prevention and protection service, and to the extent of his responsibilities, the company physician, check and assess permanent compliance with applicable provisions of law, including in connection with the outcome of the risk assessment document and any prior audit.

e) Upon completion of the checks and assessment, the employer or the holders of functions delegated by him, adopt the necessary decisions to prevent changes to equipment, systems, workplaces and the exposure to chemical, physical biological agents from jeopardizing compliance with statutory standards.

14.9 ORGANIZATION OPERATIONS

a) The employer and/or holders of functions delegated by him, executives, supervisors, RSPP, and the company physician comply with their respective obligations concerning organization operations such as emergencies, first aid, management of works contracts, periodic safety meetings, consultations with workers' safety representatives, as required of them under the paragraph LEGAL OBLIGATIONS and keep record of related activities.

b) If works inside the company are outsourced to external contractors or self-employed workers and in case of execution of agreements for agency work, the employer prepares and keeps a specific file where it includes all duly catalogued documents on compliance of provisions set out to such effect by regulations on the protection of occupational health and safety, including with reference to the contents of the relevant agreements.

c) In the event of outsourced construction works, a specific file is prepared and kept within the relevant corporate Function which includes all duly catalogued documents on compliance of provisions set out to such effect by regulations on the protection of occupational health and safety, including with reference to the contents of the relevant agreements and assignments.

14.9.1 DESIGNATION OF WORKERS IN CHARGE OF IMPLEMENTING FIRE-PREVENTION AND FIRE-FIGHTING MEASURES AND OF WORKERS EVACUATION IN THE EVENT OF SERIOUS AND IMMEDIATE DANGER, RESCUE, FIRST AID AND, IN ANY CASE, OF EMERGENCY MANAGEMENT AND DRAFTING INTERVENTION MEASURES

a) The Employer, with the support of the RSPP, designates workers in charge of implementing measures for fire-prevention and fire-fighting, evacuation of workers in the event of serious and immediate danger, for rescue, for first aid, and – in any case – for emergency management.

b) Designated workers must meet the skills and requisites required by the law to carry out the assignment and this must be recorded in the DVR.

c) The DVR must allow to trace checks on specific requisites required by applicable legislation, describe the performance of the assessment to understand skills and time availability of workers designated to a specific role, and record the official acceptance of the assignment. The constantly updated list must be annexed to the DVR.

d) The RSPP must define specific corporate procedures aimed to govern "emergency management" and "fire hazard management" and constantly monitor their appropriateness and revision.

14.9.2 EXECUTION OF AGENCY WORK AGREEMENTS, CONTRACTS FOR WORKS AND SUBCONTRACTS

a) Agreements for agency work, works contracts and subcontracts are signed by the Employer that engages the RSPP to check and ensure that "safety costs" stated therein are fair, and to verify the existence of specific provisions concerning the protection of occupational health and safety.

b) The RSPP must identify contracts and agreements in progress and these must be checked and revised by inserting appropriate clauses in the manners described above.

c) Records of agreements for agency work, works contracts and subcontracts are filed at the prevention and protection service. Agreements are monitored and, in any event, reviewed during the periodic meeting under art. 35 Leg. Dec. 81/08.

d) Specific company regulations must define the manner and contents of information that needs to be given to external companies in connection with the set of laws and requirements that a contractor that has been awarded an order must know and undertake to comply with and cause compliance with by its employees, as well as roles, responsibilities and methods to prepare the Risk Assessment document indicating measures that need to be adopted to remove risks caused by interference between workers when several companies are involved in works.

e) Specific company regulations must define the method to qualify suppliers, in consideration of the outcome of the technical-professional check con contractors, as set out in art. 26 of Leg. Dec. 81/08, of consistency between what is supplied with purchase specifications and the best available technologies with reference to the protection of health and safety.

14.9.3 KEEPING THE LOGBOOK OF INJURIES AND RECORDING "NEAR–MISSES" (OR ACCIDENTS WITH NO INJURY)

a) The Employer, with the support of the RSPP, keeps and updates the logbook of injuries.

b) He RSPP is required to draft a written report an each injury recorded in the logbook. The report records the causes of the injury, any lacks in prevention measures, corrective actions to be taken together with their planning in time and costs.

c) The report needs to be submitted to the Employer and sent to the SC.

d) The RSPP needs to file the report, pursuant to internal regulations on roles and responsibilities concerning the management of documents on health and safety management.

e) Likewise, the same procedure applies in the event of accidents with no injuries ("near–misses") and in these cases the event needs to be recorded in the specific "accident" register.

f) The RSPP compiles, updates and keeps the "accident" register, according to internal regulations on roles and responsibilities in managing documents concerning health and safety management.

14.9.4 CONTROL OF ACCESS TO PREMISES

a) The Employer, with the support of the RSPP, defines a company policy on "Control of access to premises" aimed at regulating third party accesses to Company premises.

b) Company regulations also set out the information and training that needs to be given in the event of accesses and relevant responsibility, and Individual Protection Devices that need to be supplied to and used by visitors that access Company premises.

14.10 HEALTH SURVEILLANCE

The Employer and/or the holders of functions delegated by him and the company physician comply with obligations on health surveillance as required of them by the paragraph LEGAL OBLIGATIONS, and keep record of any relevant activities.

14.11 INFORMATION AND TRAINING

a) The Employer and/or the holders of functions delegated by him, executives, supervisors, the RSPP and, to the extent of their responsibility, the company physician comply with workers' information and training obligations, as required of them by the paragraph LEGAL OBLIGATIONS, and keep record of any relevant activities le relative.

b) Training activities are planned and performed in accordance with the provisions of the specific procedure on training management[28].

14.12 SAFE WORK PROCEDURES AND INSTRUCTIONS

a) The Employer and/or the holders of functions delegated by him, executives, and supervisors comply with their obligations to supervise compliance with safe work procedures and instruction by workers, as required of them by the paragraph LEGAL OBLIGATIONS, and keep record of any relevant activity.

b) Upon completion of the surveillance activity stated in point a) above, the employer and/or the holders of functions delegated by him, executives, and supervisors take all decisions necessary to ensure workers' compliance with safe work procedures and instructions, and keep record of any action they take.

14.13 REQUIRED DOCUMENTS AND CERTIFICATES

a) The Employer and/or the holders of functions delegated by him, executives, the RSPP, and the company physician comply with the obligation to acquire documents and certifications required by the law, as required of them workers, and keep record of any related activity.

b) Any obtained documents and certificates required by law are filed and kept by the relevant corporate functions.

14.14 SPECIFIC PROCEDURAL PRINCIPLES

The Employers, with the support of the RSPP and, to the extent of their responsibility, the Company Physician formalize and revise:

[28] Procedure PGS-04 Training

- procedures[29] that:
  - → require systems to record that the activities listed in para. 1 of Art. 30 of Leg. Dec. No. 81/08 were completed;
  - → are officially notified to all persons required to comply with them and thus become binding for them, since no compliance may trigger disciplinary penalties under the Discipline Code already adopted to such effect by the Company;
  - → are under constant monitoring by the SC;
- company regulations to ensure that control of activities, implementation of preventive action, monitoring of data on safety, maintenance management, occupational health and safety audit management, management of communication between the different functions, system review, health surveillance management, are consistnet with legislation.

14.14.1 INDIVIDUAL PROTECTION DEVICES (DPI)

The Employer, with the support of the RSPP, defines company regulations to manage, distribute and maintain efficiency of Individual Protection Devices for workers and for technical services staff[30].

Company regulations define the methods to establish the presence of the necessary requisites such are resistance, appropriate and maintained state of preservation and efficiency of the DPIs. They require traceability of delivery of DPIs and the check of their proper operation (e.g. targeted checklist such as lists of individual protection devices to deliver, shared with the RSPP).

[29] These include, but are not limited to: “Risk assessment”, “Training management”, management of “medical checkups”.

[30] Procedure “PGS-10 DPI management”

14.15 TRACEABILITY

All performance of requirements in this policy are fully recorded by the parties that are responsible for them.

All documents are filed by the relevant corporate functions and are filed in the Company areas to which they belong[31].

[31] "Document management" procedure.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION E
Offenses in the field of Industrial Property and Copyright or Offenses of Disruption of Competition

15. OFFENSES IN THE FIELD OF INDUSTRIAL PROPERTY AND COPYRIGHT / OFFENSES OF DISRUPTION OF COMPETITION

15.1 CASES OF OFFENSES IN THE FIELD OF INDUSTRIAL PROPERTY AND COPYRIGHT OR DISRUPTION OF COMPETITION

This Special Section refers to offenses in the field of industrial property and copyright and disruption of competition.

This section concerns individual offenses described in Arts. 25 bis (with regard to predicate offenses as set out in Arts. 473 and 474 of the Criminal Code), 25-bis.1, 25-novies in Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

15.2 CONNECTION OF THE SPECIAL SECTION "CYBERCRIME AND ILLEGAL DATA PROCESSING" WITH THE OFFENSES IN ART. 25-NOVIES OF LEG. DEC. 231/01: OF COPYRIGHT

With reference only to predicate offenses concerning copyright in art. 25-novies deriving solely from an incorrect use of IT resources, including but not limited to:

- reproduction or reuse of the content of databases;
- illegal duplication, reproduction, transmission or public broadcasting of intellectual works destined to television or cinema distribution;
- uploading to a system of IT networks, on any type of connection, all or part of an intellectual work protected by copyright,

the Special Section on Art. 24-bis of Leg. Dec. 231/2001 on "CYBERCRIME AND ILLEGAL DATA PROCESSING", albeit stating that the two types of offenses (Art. 24-bis and 25-novies of Leg. Dec. 231/01) protect different legal interests, is an additional protection against such offense because:

- both types have a common assumption: users' correct use of IT resources and ethical principles;
- areas of risk, as a consequence of such circumstance, partially overlap;
- procedural principles aim, in both cases, to ensure awareness in Addressees on the numerous consequences from an incorrect use of IT resources.

15.3 SENSITIVE PROCESSES IN CONNECTION WITH OFFENSES IN THE AREA OF INDUSTRIAL PROPERTY AND COPYRIGHT AND DISRUPTION OF COMPETITION

With reference to the offenses under Art. 25 bis (with regard to predicate offenses as set out in Artts. 473 and 474 of the Criminal Code), 25-bis.1, 25-novies, theoretically risk-featuring sensitive processes are:

A. INTELLECTUAL PROPERTY

1. Managing corporate agreements with respect to elements that are relevant for intellectual property:
    - Intellectual property license agreements
    - Procurement and logistics agreements
    - Distribution agreements
2. Managing IP litigation
3. Managing external consultants: trademark/patent consultants, engineering companies
4. Managing IP training activities

B. COPYRIGHT

1. Managing corporate agreements with respect to elements that are relevant for copyright:
    - Copyright license agreements where the Company is licensor or licensee
    - Procurement contracts for works covered by copyright
    - Distribution agreements for works covered by copyright
2. Managing copyright litigation
3. Managing external consultants on works covered by copyright
4. Managing training on copyright

C. DISRUPTION OF COMPETITION

1. Managing corporate agreements with specific respect to:
    - Business partnership agreements (joint ventures, consortiums, etc.)
    - Procurement/distribution agreements
    - Engagements to advertising/communication agencies
2. Managing unfair competition litigation
3. Managing product production, packaging and sale
4. Managing corporate procedure on pricing
5. Managing training on law and competition practice
6. Managing marketing policies
7. Managing business strategy and development plans (in terms of expansion of the geographic market and product of reference);
8. Managing purchase operations relating to the sale of products bearing registered trademarks or patented products.

Involved corporate roles:

- CEO;
- Commercial Director, Retail Managers;
- Product Director, Product Managers, Technical Services Manager, Sourcing Manager;
- Marketing Manager, Branch Merchandising & Administration Manager, IT Manager, Merchandising Manager, Logistic Manager.

15.4 GENERAL PRINCIPLES OF CONDUCT

The following general prohibitions apply to Corporate Bodies, executive and Employees directly, while they apply to consultants, suppliers and partners under specific contract clauses.

These parties are prohibited from adopting, participating in or causing the adoption of conducts which, taken individually or collectively, directly or indirectly qualify as the offenses listed above. Breaches of the corporate principles and procedures described in this Special Section are also prohibited.

In accordance with the provisions of the Code of Ethics, corporate procedures, policies and regulations include, by way of example, the following prohibitions for the parties identified above:

- Unauthorized installation and use of software on company hardware and systems, and in any case the use of unlicensed software in performing any activities in the interest or on behalf of CONBIPEL S.p.A.;
- Purchase, sale, distribution, storage, holding and howsoever managing assets protected by copyright or intellectual property rights without prior check that CONBIPEL S.p.A. acquired the relevant licenses or necessary authorizations;
- Purchase, sale and in any case management of services protected by intellectual property rights without prior check that CONBIPEL S.p.A. has the necessary authorizations;
- Manufacture, packaging, purchase, sale and in any case management and marketing of products bearing counterfeit or false signs;
- Definition of business cooperation agreements of any kind whose purpose is to disrupt competition or which, in fact, generate such effect;
- Manufacture, packaging and sale of products capable of disrupting competition.

15.5 SPECIFIC PROCEDURAL PRINCIPLES

Addressees are prohibited from:

a. Preventing or disrupting the operation of industry or trade by using violence on things or using fraudulent means;

b. Delivering purchasers a mobile object for another or a mobile object by origin, quality or quantity that is different from what was stated or agreed on;

c. Selling or howsoever distributing intellectual works or industrial products with domestic or foreign names, trademarks or distinctive signs capable of misleading the purchaser on the origin or quality of the works or products[32];

d. Carrying out acts of competition using violence or threat;

e. Placing on sale or distribution on domestic or foreign markets, industrial products with counterfeit or infringed names, trademarks or distinctive signs;

f. manufacturing or using industrially objects or other assets made by appropriating or infringing industrial property rights.

15.6 TRACEABILITY

Performance of all requirements in this policy are appropriately recorded by the parties that are responsible for them.

Traceability is also ensured by filing process documents electronically.

All documents are recorded by the persons responsible for them and are filed by the relevant corporate function.

[32] In accordance with the specific paragraph in the Procedure "Managing Activities for the Purchase of goods and Services related to the product".

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION F
Counterfeit Money and Counterfeit Distinctive Signs

16. COUNTERFEIT MONEY AND COUNTERFEIT DISTINCTIVE SIGNS

16.1 CASES OF COUNTERFEIT MONEY, SECURITIES, OFFICIAL STAMPS AND DISTINCTIVE SIGNS OR MARKS (ART. 25 BIS LEG. DEC. 231/2001).

This Special Section concerns the offenses in Art. 25 bis Leg. Dec. 231/2001.

Individual offenses considered are the ones described in Art. 25 bis (with regard to predicate offenses and set out in arts. 453, 454, 455, 456, 457, 459, 460, 461, 464, 473 and 474 of the Criminal Code) in Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

16.2 SENSITIVE PROCESSES IN THE AREA OF COUNTERFEIT MONEY, SECURITIES, OFFICIAL STAMPS AND DISTINCTIVE SIGNS OR MARKS

The following sensitive processes emerged in connection with the offenses of counterfeit money, securities, official stamps and distinctive signs or marks:

- Managing cash collections and cash payments.

Involved company roles:

- CEO;
- CFO, Treasury Manager, Financial Control, Accounting & Administration Manager, Import Manager;
- Commercial Director, Retail Managers, Real Estate Manager, Business Operation Control Manager.

16.3 GENERAL PRINCIPLES OF CONDUCT

It is prohibited to adopt, take part in or cause the adoption of conducts which may fall under the offenses considered in Article 25-*bis* of the Decree.

Breaches of the corporate principles and procedures stated in this Special Section are also prohibited.

In connection with the above conducts, it is especially prohibited to disseminate, including as accomplice, counterfeit currency.

Users that receives currency in good faith and then have doubts on its lawfulness must not, in turn spend it, because this behavior is an offense. In these cases, the bank bill must be shown to experts as soon as possible, such as ordinary tellers of banks or post offices or the Bank of Italy.

Based on provisions applicable in Italy, banks and other parties that handle or distribute bank bills professionally are required to remove from circulation any bank bill that they consider counterfeit and send it to the local branch of the Bank of Italy.

16.4 SPECIFIC PROCEDURAL PRINCIPLES

Addressees of this Model are required, where involved in the process of managing valuable assets, to comply with the following rules of conduct:

a. Anyone handling payments in cash is required to monitor cashed bank bills to identify any counterfeit currency. The identification activity may also occur with bank bill selection and acceptance equipment, or legal checks by trained staff with manual procedures;

b. If Employees have doubts on the regularity or genuine nature of a bank bill that they received, they must not attempt to recirculate it. This behavior would trigger a criminally punished offense. The bank bill must be put aside and be examined by the tellers of banks with which the company does business or of post offices or branches of the Bank of Italy;

c. Any Employees entrusted by the Company to deliver doubtful bank bills to authorized institutions shall have these entities deliver a receipt that shall be duly kept in the Company's records;

d. Addressees must refrain from counterfeiting, altering or using distinctive signs of intellectual works or counterfeit or altered industrial products;

e. Addressees must refrain from introducing in Italy for trade, selling or however putting into circulation intellectual works or industrial products with Italian or foreign counterfeit or altered trademarks or signs.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION G
Cybercrime and Illegal Data Processing

17. CYBERCRIME AND ILLEGAL DATA PROCESSING

17.1 CASES OF CYBERCRIME AND ILLEGAL DATA PROCESSING

This Special Section concerns cybercrime and illegal data processing.

Individual offenses covered are described in Art. 24 bis Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

17.2 SENSITIVE PROCESSES IN THE AREA OF CYBERCRIME AND ILLEGAL DATA PROCESSING

17.2.1 RISK-FEATURING AREAS

In connection with the offenses and criminal conducts in the scope of cybercrime and illegal data processing, areas regarded as featuring risks are:

i. All corporate businesses through company IT systems, email and internet access;

ii. Management of company IT systems to ensure the operation and maintenance, the evolution of the IT technological and application platform, and IT security;

iii. Management of electronic IT flows with government agencies;

iv. Use of software and databases;

v. Management of contents of the website.

Addressees of this Special Section in general are:

- Staff designated to develop, install, service and maintain applications and technological infrastructure;
- Staff in charge of managing data in accounting and IT systems in general.

Tasks assigned to System Administrators – with a written designation document – are monitored through the adoption of measures set out by the Italian Data Protection Authority by keeping record of administrative logs for 180 days.

Cybercrime committed by system administrators do not require charges filed by the party, as these may be prosecuted ex officio by the authorities.

In drafting this Model, we assessed the management of required log files under the regulations set by the Italian Data Protection Authority on system administrators' accesses and email log files.

17.2.2 SENSITIVE ACTIVITIES

The following sensitive processes emerged:

- Organization and Size of IT, software and hardware system management, network services management and protection;
- Accesses and Authorizations (managing and monitoring accesses to ITC systems, managing user profiles and authentication processes, managing physical access to sites which host IT facilities, managing and protecting workstations);
- Workstation Security;
- Certifications and statutory requirements;
- Control and Vulnerability Assessment of the IT System and management of outgoing accesses;
- Application Functionality Design (application software, using and managing corporate data with IT tools with standard business software and/or corporate management platform)

Involved company roles:

- CEO;
- CFO, Financial Control, Accounting & Administration Manager;
- IT Manager.

17.3 GENERAL PRINCIPLES OF CONDUCT

17.3.1 GENERAL PRINCIPLES

The following general principles apply to Addressees that is everyone to the extent that they are involved in carrying out operations that are included in risk-featuring areas and based on their respective positions or requirements undertaken with the Company.

Specifically, this Special Section intends to:

a) List general principles and specific general principles that Addressees are required to follow to correctly apply the Model;

b) Give the SC and managers of corporate functions called to cooperate with it operating principles and tools necessary to carry out the checking, monitoring and auditing activities for which it is designated.

In carrying out their functions/activities, in addition to the rules in this Model, corporate officers are generally required to comply with all the rules and principles in the sections that concern them in following documents:

1. Organization chart and organization diagrams;

2. Control of logic access to IT resources by making access codes and passwords personal and confidential;
3. Internal password management procedures changing passwords as required without conceiving methods to avoid security logic;
4. Period check of required log files by system administrators (access by system administrators and email);
5. Periodic audit, including through external experts supporting the SC, to assess the application of this Organization Model and to sample check conducts involving IT tool use;
6. Periodic assessment of the level of IT Security that by nature decreases in time, if appropriate investments are not made;
7. Periodic audit of investments in IT, with specific reference to the update of tools, including network tools, and software.

17.3.2 GENERAL PRINCIPLES OF CONDUCT

Major purposes of IT security are:

- **Confidentiality**: to ensure that data is preserved from improper accesses and is used solely by authorized persons. Confidential information is protected in transmission and saving/storing, so that information is accessible only by persons that are authorized to know it;
- **Integrity**: to ensure that all corporate data is actually the one that was entered in the IT system and was modified only legitimately. To ensure that information is processed in a manner that it cannot be tampered with or altered by unauthorized persons, and however, in case of tampering, the author may be identified;
- **Availability**: to ensure the availability of corporate data based on the needs of process continuity and in compliance with regulations that required historical archives.

Based on these general principles, Corporate Bodies, Employees and Partners (to the extent of requirements in specific procedures and obligations in specific contract clauses) are prohibited from:

- Adopting, cooperating or causing the adoption of conducts that may individually or collectively qualify as the offenses included in the category under review (art. 24-bis of Leg. Dec. 231/2001);
- Breaching corporate principles and procedures in this Special Section.

Within such rules, it is especially prohibited to:

a) Alter public or private IT documents having the effects of evidence;

b) Improperly access the ICT system of the Company or government entity or private third parties;

c) Improperly access ICT systems to alter and/or delete data and/or information, or to steal them to reuse them in competing businesses and to the advantage of the Company;

d) Improperly hold and use codes, passwords or other appropriate access means to an ITC system of government entities or private competitors to acquire confidential information. Network users are requested to report without delay the existence of these situations;

e) Improperly hold and use codes, passwords or other appropriate access means to the Company's ITC system to acquire confidential information;

f) Carry out procurement and/or manufacturing and/or equipment and/or software distribution activities to damage an ITC system of government entices or private parties, any information, data or programs contained in them, or to favor full or partial interruption or alteration of their operation;

g) Carry out fraudulent activities to intercept, prevent or interrupt communications related to an ITC system of government entity or private parties to acquire confidential information;

h) Install equipment to intercept, prevent or interrupt communications of government entities or private parties;

i) Carry out activities to modify and/or delete data, information or programs of government entities or private parties or in any event useful to the public;

j) Carry out activities to damage other parties' information, data and ITC programs;

k) Destroy, damage or make any ITC systems useful to the public unfit for use;

l) Acquire, distribute, sell or hold for business or entrepreneurial purposes programs on media that does not bear the SIAE mark, works protected by copyright or pirated databases and software;

m) install or use unauthorized software protected by copyright that is not installed by internal technical staff, for any work task and to manage data owned by the Company;

n) in general, all use of IT systems for purposes that are incompatible with the ones for which they are assigned to users is prohibited. Specifically, it is prohibited to:

    a. use IT systems to play games;

    b. download, upload or install unauthorized software (music, films, photo, programs, etc.) and, however, in breach of copyright;

c. use removable tools (such as USB memory sticks) that were not controlled beforehand and in any case these must be used only for tasks that are related to working activities;

d. disclose, howsoever, to unauthorized third parties, or howsoever enable them to know data, information, formulas, process descriptions, documents, materials of any nature that is confidential or the knowledge of which by third parties could damage the Company;

e. howsoever produce, hold or disseminate pornographic and child-pornography material, material for the propaganda or inducement to terrorism, or offensive for the honor and dignity of third parties;

f. Breach IT registers and archives of the Company and/or falsify data, information or documents of any kind;

g. Notify to third parties, transfer, transmit, disclose or make available, in any form or manner, and for any reason whatsoever, access passwords to the Company's or third parties' IT systems that are known to the addressees of the procedure because of their activity.

Therefore, the persons listed above, and Employees specifically, must comply with the following principles:

1. General principles:
    - IT systems must be used in strict compliance with applicable legislation, especially according to the measures adopted under the European GDPR Regulations and the Code of Ethics in force;
    - The Company complies with all Privacy regulations, according to the European GDPR, which all directors, employees and independent contractors respect;
    - All software installed on the Company's systems have regular licenses and no one is authorized to remove, reinstall or modify such software;
    - Each user is personally responsible for the (physical and functional) integrity of systems and of relevant data, information and programs, and their custody when transferred outside the company premises (mobile devices) where they can be stolen to acquire Company data.
2. As to operations concerning the management of accesses, accounts and profiles and the management of software systems, policies set out that:
    - The process is formalized by an internal operating procedure/policy;
    - System authentication requisites to access data and to assign remote access to such systems for third parties, such as consultants and suppliers, are officially defined;
    - User-ID for application and network access are individual and unique:

  - Access to each ITC systems is restricted to one or more users identified by surveillance of premises and by the use of logic keys (user-ID and password) and physical keys (doors to rooms are locked);
  - Each User-ID matches a profile to access corporate networks and the internet (where applicable). Each profile matches access to applications, access restrictions to the corporate IT system (form), and related tasks (display, data entry, modifying entered data);

- Correct password management was defined by guidelines disclosed to all users for the selection and use of passwords:
  - Assignments of ITC systems or User-IDs for use are requested by function managers and must be disabled immediately upon termination of employment, always upon request of the function manager;
  - Assignments of ITC systems or User-IDs for use are requested by function managers. The request must be include reasons connected to the tasks that the user has to carry out. Assigned User-IDs are recorded and filed by the relevant IT area. Formal procedures apply for the assignment of special privileges (e.g. superuser, power-user);
  - Whenever job tasks change, the function manager of the user and/or the HR manager report the need for a profile change to the relevant System Administrator that immediately revokes the previous User-ID. User-IDs are periodically reviewed. The principles listed above apply for the assignment of new profiles;
- Criteria and methods are defined to create access passwords to: network, applications, corporate information assets, and critical or sensitive systems (e.g. minimum characters in a password, complexity rules, expiration);
- Accesses by users to data, systems and network , with any methods, are periodically reviewed;
- Each user is assigned a personal email account. The use of email through this account is for business purposes only. Incoming and outgoing emails to and from such account are addressed to and sent by a corporate function and may be used according to the guidelines of the Data Protection authority for the use of email and the internet at work GU 58 10/3/2007;
- Certified electronic signatures are used based on a specific written delegation of the Company's legal representative;
- Applications keep track of changes to data by uses;
- Criteria and methods to assign, change and delete user profiles are defined; in the event of the user's termination of employment with the Company or change of job tasks, passwords and User-IDs of the Company's IT systems are revoked; the Company will be responsible for informing external entities whose

passwords and related User-IDs may be known to such user on behalf of the Company;

- Organization roles are defined in an authorization matrix: applications / profiles / person making the request;
- User profiles are checked periodically to determine that they are consistent with assigned responsibilities;
- Record is kept of documents concerning each activity to ensure full their full traceability;
- The Company may also revoke, fully or in part, the use of IT systems or prevent, fully or in part, access to corporate or other IT networks, by one or more users (for instance, using filters);
- Criteria and methods are defined to manage software systems that involve the compilation and maintenance of an updated inventory of software in use by the Company, the use of officially authorized and certified software, and completion of periodic checks on installed software and on system mass memories in use to establish if prohibited and/or potentially harmful software is present;
- Criteria and methods are defined for change management (meaning updating and implementing new systems/technological services);
- A business continuity plan is defined and periodically updated and tested.

3. Operations concerning the management of hardware systems, of physical accesses where IT facilities are located, and of network services, policies require that:
    - Criteria and methods for the management of hardware systems require the compilation and maintenance of an updated inventory of hardware in use at the Company premises and govern responsibilities and operating methods for hardware implementation and/or maintenance;
    - Criteria and methods for backup operations determine, for each hardware application, the frequency of the task, the procedure, the number of copies and the data conservation period;
    - Record of the documents concerning each task has to be kept to ensure full traceability;
    - Security measures are defined as are and surveillance methods along with their frequency, their responsibility, the reporting process for any trespassing in technical rooms or breach of security measures, any countermeasures to implement;

- Credentials for physical access to sites where IT systems and IT infrastructures are located are defined, including but not limited to access codes, PINs, badges and their traceability;
- responsibilities for network management are defined;
- security checks are implemented to ensure confidentiality of internal network data and data in transit on public networks;
- mechanisms are adopted to segregate networks and to monitor network traffic;
- mechanisms are implemented to trace security events on networks (such as non-standard accesses by frequency, method, time);
- IT network implementation and maintenance are regulated by defining responsibilities and operating procedures, periodic operation checks on networks and on detected anomalies; also, periodic vulnerability assessment and ethical hacking tasks must also be regulated;
- Criteria and methods for backup tasks must indicate, for each telecommunication network, task frequency, procedure, number of copies and data conservation period.

As to operations concerning digital document services and management, policies require that:

- The process is formalized in an operating procedure or internal policy;
- Criteria and methods are defined to generate, distribute, revoke and file keys (smart cards);
- The management, if any, of digital documents by third parties is officially regulated;
- Checks are defined to protect smart cards from possible changes, destruction and unauthorized use;
- Documents supporting tasks completed by sending digital documents may be traced and appropriate records are kept.

17.4 SPECIFIC PROCEDURAL PRINCIPLES

For the sake of completeness and to provide operating details of the principles stated in the Code of Ethics, specific polices were formalized (*Group policies, policy for the management of IT systems*) that, in addition to clearly defining roles and responsibilities of parties involved in the process, also define a set of specific and material controls to mitigate risk factors.

The Company is also committed to:

1. Appropriately informing Employees, and interns and other persons (such as Partners) possibly authorized to use IT systems of the importance of:
   - Keeping one's credentials confidential and refraining from disclosing them to third parties;
   - Using available software and databases correctly;
   - Refraining from adding data, images or other material protected by copyright without obtaining the necessary authorizations from one's hierarchical superior according to the indications in corporate policies;
2. Arranging periodic training sessions for Employees, diversified based on job duties and, to a lesser extent, to interns and other parties (such as Partners) possibly authorized to use IT systems, to spread the clear awareness of risks from improper use of the Company's IT resources;
3. Having Employees and interns and other parties (such as Partners) possibly authorized to use IT systems sign a specific document whereby they undertake to use correctly corporate IT resources and safeguard them.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION H
Organized Crime

18. ORGANIZED CRIME

18.1 CASES OF ORGANIZED CRIME

This Special Section concerns organized crime.

Individual offenses are described in Art. 24 ter Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

18.2 SENSITIVE PROCESSES IN CONNECTION WITH ORGANIZED CRIME

The offenses in Art. 24-ter of the Decree cannot apparently be connected with specific activities actually performed by the Company. Moreover:

- These offenses, for the most part, involve associative offenses (conspiracy to commit crimes, mafia-type including foreign mafia conspiracy) or strongly connected with associative offenses (political-mafia vote buying, crimes committed by using the methods described in art. 416-bis of the criminal code or to support the activity of the associations listed in such article), which punish only the mere agreement of several persons aimed at committing an undetermined number and type of crimes;
- Association offenses, by definition, consist in an agreement aimed to perpetrate any offense and as such expand the set of predicate offenses to an undetermined number of crimes, so any activity carried out by the Company could trigger perpetration of an offense – and the consequent responsibility under Leg. Dec. 231/2001 – "through" a conspiracy to commit crimes.

However, even if such offenses are, as stated above, not connected to specific operations actually performed by the Company – and accordingly to its operating procedures – they may nonetheless theoretically be committed by Top Managers and Subordinates. In relation to this aspect, the prevention system already implemented within the Company is significant.

We are of the opinion that, to prevent these crimes, already implemented corporate policies already serve as appropriate prevention, as do the principles in the Code of Conduct, which are the most effective tool for offenses such as conspiracy to commit crimes under Art. 416 of the Criminal Code, because it is impossible to frame within a specific control system the nearly infinite number of conducts that could be committed through an association bond.

Nonetheless, the Company has identified a series of tasks where parties connected with criminal association, or that however carry out illegal business, could come into contact with and operate enterprises with the Company. Specifically, the following sensitive activities were identified, where potentially some of the offenses of organized crime in Art. 24-ter of the Decree could be committed:

- Managing relations with contractors, subcontractors and suppliers of goods and services.
- Managing taxes, including through external consultants.
- Managing collection, storage and disposal of waste, including through outsourcers.
- HR selection and recruitment.
- Managing reporting concerning state subsidies.

Company roles involved:

- CEO;
- CFO, Treasury Manager, Financial Control, Accounting & Administration Manager, Human Resources Manager, Import Manager;
- Commercial Director, Retail Managers, Real Estate Manger, Business Operation Control Manager;
- Marketing Manager, Logistic Manager.

18.3 GENERAL PRINCIPLES OF CONDUCT AND SPECIFIC PREVENTION POLICIES

Given the specific nature of offenses such as conspiracy to commit crime under Art. 416 of the Criminal Code, which imply the impossibility to frame within a specific control system the nearly infinite number of conducts that could be committed through an association bond, the general principles of conduct to prevent such offenses, which are the most appropriate tool, are set out in the Code of Ethics.

Specific prevention Policies are in any case indicated in connection with individual sensitive activities, in the scope of which some of the offenses referred to in the previous paragraph could potentially be committed,

a) **In case of operations concerning the management of relations with contractors, subcontractors and suppliers of goods and services and the management of the collection, stocking and disposal of waste, including through outsourcers, policies require**:

- Relations with contractors, subcontractors and suppliers must be governed by a written contract that clearly indicates the value of the transaction or the criteria to determine such value;
- In selecting contractors, subcontractors and suppliers for the collection, stocking and disposal of waste, the Company must request anti-mafia substitute declaration;

- In selecting the third party, its reputation and reliability on the market are assessed beforehand, as is its adoption of values that are consistent with the Company's Code of Conduct and Model;
- If the third party refuses to sign contract clauses on acceptance of the principles in the Model and Code of Conduct the Company will terminate the agreement or prevent its execution;
- The selection and assessment of suppliers and contractors / subcontractors must be based on criteria that were predetermined by the Company; such criteria need to be reviewed and, where appropriate, revised on a regular basis. The Company must periodically test the effectiveness of such criteria in detecting anomaly indicators with respect to organized crime;
- The manager of the function involved in the transaction must immediately report to the Surveillance Committee any anomaly in services rendered by the third party, peculiar requests submitted to the Company or the third party's involvement in penalties set out in Leg. Dec. 231/2001.

b) **In case of operations concerning the management of taxes, including through external consultants polices require:**
   - That invoices received and issued by the Company for the purchase of goods and services are checked to determine the existence of the transaction and their amount as stated in the document, that they are consistent with agreements, purchase orders or order confirmation of the Company, as per the Procedure "Management of purchases of product-related goods and services".

c) **In case of transactions concerning the selection and recruitment of staff,** reference should be made to specific prevention policies on HR.

d) **In case of transactions concerning reporting related to government subsidies,** reference should be made to specific prevention policies concerning this area.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION I

Incitement to Refrain From Making Statements or to Make False Statements to the Judicial Authority

19. INCITEMENT TO REFRAIN FROM MAKING STATEMENTS OR TO MAKE FALSE STATEMENTS TO THE JUDICIAL AUTHORITY

19.1 CASES OF INCITEMENT TO REFRAIN FROM MAKING STATEMENTS OR TO MAKE FALSE STATEMENTS TO THE JUDICIAL AUTHORITY

This Special Section concerns the offense of incitement to refrain from making statements or to make false statements to the judicial authority, under Art. 377-bis, of the Criminal Code.

Individual cases of offenses are described in Art. 25-decies Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

19.2 PREVENTION

The offenses in Art. 377-bis of the Criminal Code are not connected to specific business operations of the Company and cannot be framed in a specific system of controls, since they could be committed at any Company level and in a nearly infinite number of manners.

The principles in the Code of Ethics are the most appropriate tool to prevent perpetration of the offenses of inciting to refrain from making statements or to make false statements to the judicial authority.

So, to prevent conducts capable of triggering this type offenses, all Addressees of the Model adopt practices and behaviors that are in compliance with the Code of Ethics. Specifically, Addressees of the Model follow the ethical principles of the Company concerning relations with other parties, whether Company staff or third parties.

19.3 SPECIFIC PROCEDURAL PRINCIPLES

It is prohibited for Addressees to:

a) Incite third parties not to make statements to the judicial authority;

b) Incite third parties to make false statements to the judicial authority.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION L
Environmental Crime

20. ENVIRONMENTAL CRIME

20.1 CASES OF ENVIRONMENTAL CRIMES

This Special Section refers to environmental crime that are significant for CONBIPEL, for its administrative premises, its central warehouse and the store network.

Individual cases of offense are described in art. 25-*undecies* of Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

20.2 FUNCTION AND ADDRESSEES

This Special Section concerns conducts adopted by Corporate Bodies, Employees, and Consultants and Partners, as defined in the General Section. The goal of this Special Section is that the persons listed above maintain conducts that are in line with the principles described below, to prevent perpetration of the offenses listed in the previous paragraph.

Specifically, this Special Section serves the purpose of:

a) Providing a list of general principles and specific procedural principles that Addressees are required to comply with to correctly apply the Model;
b) Providing the SC and the Company's function managers that cooperate with it with the principles and operating tools necessary to exercise its control, monitoring and audit operations.

In performing the relevant activities/functions, in addition to laws specific to this area and the rules in this Model, Addressees are required, in general, to comply with all rules and principles stated in the following documents, with respect to the sections that pertain to them:

- Company charts, along with the specific identification of assigned tasks and functions
- CCNL
- Code of Conduct

With reference to environmental regulations:

- Legislative Decree No. 121/2011
- Legislative Decree No. 202/2007
- Legislative Decree No. 152/2006, as subsequently amended and supplemented
- Law No. 549/1993
- Law No. 150/1992
- Art. 452-bis, Criminal Code, Environmental pollution
- Art. 452-quater, Criminal Code, Environmental Disaster
- Art. 452-quinquies, Criminal Code Offenses against the environment with no willful intent
- Art. 452-sexies, Criminal Code Trafficking and abandonment of highly radioactive material
- Art. 452-octies, Criminal Code, Aggravating circumstances
- Art. 452- quaterdecies, Criminal Code, organized activities for illegal waste trafficking

- Art. 727-bis, Criminal Code, The killing, destruction, catching, possession or taking of specimens of protected wild fauna or flora species
- Art. 733-bis, Criminal Code, Destruction or deterioration of a habitat within a protected site
- Procedures, Guidelines, Operating instructions adopted by CONBIPEL in compliance with environmental regulations
- Any other internal regulation adopted by CONBIPEL in connection with the environmental control system or capable, howsoever, of having an impact on it, including indirectly.

In light of the different positions and different obligations that each Addressee has with CONBIPEL in carrying out risk-featuring tasks, this Special Section expressly prohibits Addressees from adopting, promoting, cooperating in or causing conducts capable of qualifying as offenses committed in breach of environmental regulations.

Accordingly, the following elements are specified:

a) Activities and/or processes defined as "sensitive" meaning featuring risks of an offense being committed;
b) The fundamental principles of reference, the implementation of which requires adoption of specific procedures, with a view to the correct application of the Model;
c) Principles of reference that will have to inspire control, monitoring and audit operations of the SC and of the managers of corporate functions that cooperate with it, duly set out in specific internal policies that need to be adopted for the Model to be correctly applied.

20.3 GENERAL ISSUES

CONBIPEL does not have environmental systems that are certified to the international standard UNI EN ISO 14001.

Environmental monitoring of corporate operations allows to prevent and mitigate risks by planning self-monitoring and potential surveillance operations by an auditor of the corporate department.

Maintaining compliance with the law in the area of the environment is ensured by compliance with Procedures and Policies prepared to such effect, which are constantly revised to account for changes in legislation and in the corporate structure.

Organizing these controls implies the use of calendars that are shared by several internal resources, managed by the Delegated Safety Executive, and also requires periodic coordination and planning meetings.

At administrative offices, central warehouse and stores, qualified suppliers carry out periodic control activities on the refrigeration circuit of air-cooling and conditioning systems to ensure compliance with requirements on protection of stratospheric ozone applicable to CONBIPEL and when it acts as lessors or lessee of the real estate property or of the line of business.

20.4 SENSITIVE PROCESSES IN THE AREA OF ENVIRONMENTAL CRIME

With reference to the offenses under art. 25 *undecies*, the following sensitive processes emerged:

1. **Identifying environmental impacts and managing objectives, goals and programs**;

2. **Managing regulatory obligations to be complied with and managing environmental documents**;

3. **Managing legal obligations on liquid waste discharges**:

- No special discharge of waste water was identified because there are no corporate processes that generate industrial waste water capable of theoretically generating pollution in underground water; therefore, generated waste water is similar to home waste water
- Discharge in the soil, in the superficial layers of subsoil, in subsoil and in underground water, in connection with leaks of substances from batteries/storage cells of fork lifts
- Discharge in the soil, in the superficial layers of subsoil, in subsoil and in underground water, in connection with leaks of hydraulic fluid from fork lifts

4. **Implementation of statutory requirements on waste management:**

- Managing production, classification, collection, storage and disposal of production waste during standard operations, at the headquarters, warehouse and stores
- Waste generated during building renovation of stores
- Managing production, classification, collection, storage and disposal of WEEE
- Managing Sistri records and managing documents required by the law (forms, certificates, Mud, etc.)
- Managing waste transportation and disposal operations through authorized outsourcers
- Managing operations concerning temporary storage at the production site of dangerous waste from healthcare activities with reference to the disposal of expired products on stock in first aid kits installed at Company premises or waste generated further to a first-aid action (limited to para. 2 lett. b) item 1 of Leg. Dec. 231/2001 or Art. 256, para. 6/1 of Leg. Dec. 152/2006: “Failure to comply with the requirements in Art. 8 of Pres. Dec. 254/2003 in temporary storing at the production site dangerous waste from healthcare activities (labelling, type of container, disposal entry times, recording times)”).

5. **Implementation of statutory requirements on the management of air emissions:**

- Air emissions above the thresholds that simultaneously exceeded air quality limit values in connection with heating systems (for all facilities where CONBIPEL is the owner of the real-estate property, while where it is the lessee performance is a responsibility of the lessor);
- Gas emissions generated during the process to recharge batteries/storage cells of fork lifts.

6. **Implementation of statutory requirements on the management of ozone depleting substances**

7. **The killing, destruction, catching, possession or taking of specimens of protected wild fauna or flora species in connection with leather-wear**

8. **Emergency management**

9. **Managing non compliances**

10. **Managing information or an information flow that makes duly empowered parties knowledgeable of situations that occurred and are relevant in connection with environmental regulations**

11. **Formalization of roles and remit, and related management responsibilities**

12. **Appropriate information and training of workers**

13. **Supervision on compliance with environmental procedures and instructions**

14. **Obtaining required authorizations and certifications and checking relevant deadlines**

15. **Periodic internal checks on the application and effectiveness of adopted procedures**

16. **Appropriate control systems on maintaining in time appropriate conditions of adopted environmental measures and record keeping of completion of the activities listed above**.

Involved company roles:

- CEO;
- Commercial Director, Retail Managers;
- Logistic Manager.

No sensitive process emerged with reference to cleanup operations, except for some minor checks on the possible presence of asbestos.

Offenses of pollution caused by watercraft and offenses related to the trade/holding of endangered flora and fauna or wild animal species were assessed as not applicable to CONBIPEL.

20.5 GENERAL PRINCIPLES OF CONDUCT

The Company adopted specific procedures to take and implement decisions in risk-featuring environmental areas. The relevant documents must be constantly updated by the responsible management or upon proposal of the Surveillance Committee.

In performing the sensitive activities, in general everybody must:

a) Operate in compliance with domestic and EC environmental laws;
b) Draft and keep records of all documents required by the law or by administrative authorizations for the operation of working activities;
c) Check and keep record of all environmental authorizations of third parties with which the Company cooperates for activities that may have an impact on the environment or are subjected to the regulations in Leg. Dec. 152/2006;
d) Effectively cooperate with regulatory authorities and agencies;
e) Review production processes and activities completed to minimize the environmental impact they generate, with a preference for best available technologies;
f) Comply with the Code of Ethics, with specific reference to the section that requires corporate activities to be operated in compliance with healthy environmental conditions;
g) Follow the intentions and directives of the corporate environmental policy;
h) Allow to trace completed transactions in time and highlight their authorization process, to guarantee full disclosure of choices. This requires all operations to be officially documented and that documents are filed and kept with a method that prevents any future change, unless appropriately indicated;
i) Allow access to the documents listed in the previous item only to persons entitled thereto based on internal rules, or their delegates, the Board of Directors or equivalent body, the audit company and the Surveillance Committee and/or, if expressly delegate thereto, to facilities in charge of audit activities;
j) Appropriately segregate roles and responsibilities so that those who adopt or implement decisions do not match with those who have to report transactions in accounts and with those who are required to make the audits required by the law and by internal procedures on such accounting records;
k) Assign appointments to Consultants consistently with actual corporate needs and pay fees or commissions that are fair for the services rendered to the Company and with the engagement. Fairness will be determined based on principles of reasonableness and with reference to rates and/or market practice and terms and conditions;
l) Any promotion and incentive mechanism to employees and independent contractors are in line with realistic objectives and consistent with tasks and activities carried out and with assigned responsibilities;
m) In the management of financial resources and more in general in decisions to

commit such resources, the Company employees banking institutions and financial intermediaries that apply full disclosure and fairness rules that are consistent with regulations of the European Unions;

n) Staff selection and recruiting operations are based on full disclosure and actual corporate needs and the reason for the selection and the involvement of the requesting unit is traceable;
o) Disciplinary systems apply to breaches of procedures.

The Surveillance Committee proposes any changes and supplements to the requirements in the relevant implementation procedures.
No exceptions are admitted to the procedures in the Model except for exceptional cases of urgency in determining or implementing the decision or in case of temporary impossibility with respect to procedures, provided that this is immediately reported to the Surveillance Committed and subsequently ratified by the relevant body.

20.6 SPECIFIC PROCEDURAL PRINCIPLES

The following paragraphs describe requirements that CONBIPEL has to abide by to implement relevant principles and applicable regulations on environmental compliance, with specific reference to Art. 25-*undecies* of leg. Dec. No. 231/2001.

20.6.1 MANAGEMENT OF STATUTORY REQUIREMENTS ON LIQUID WASTE

This activity requires to:

- Comply with the prohibition to discharge liquid waste in soil, subsoil and underground water;
- Make all drains accessible, except for household drains and drains treated as households, for sampling by the relevant authority for the relevant test;
- Periodically verify the correct implementation of the above requirements.

20.6.2 IMPLEMENTATION OF STATUTORY REQUIREMENTS ON WASTE MANAGEMENT

This activity requires to:

- Identify the legal “producer” which is decided for each waste producing operation based on an initial analysis of the waste production process that considers type of waste, procedure and timing of any controls. If the waste producer is an external business, CONBIPEL is required to oversee the proper management of conventional waste produced inside the site premises;
- Carry out the basic characterization of waste with the assignment of the EWC code (European Waste Catalogue), to correctly manage it on and off site, and so that waste of all categories may be accepted by the landfill. In case of doubts on the EWC code, especially for assigning hazard, carry out chemical analyses through qualified labs to correctly identify waste;

- Update loading and unloading registers upon producing and handling waste;
- Manage the temporary storage of waste according to applicable legislation;
- Manage preliminary stocking and destination to reserve of waste according to applicable authorizations;
- Fill in and issue waste identification forms for transportation off site;
- Request and verify required authorizations of all parties involved in the various steps of waste management (collection, transportation, recovery, disposal);
- Verify acceptance of the destination site by receiving the fourth copy of the form;
- Starting from the effective date of the System for the traceability of waste (SISTRI):
  - The Sistri form "Area registro cronologico", and the Sistri form "Area movimentazione" must be filled in, acceptance of the destination site must be established by receiving an email from Sistri;
  - Periodically check the proper implementation of the above requirements.

20.6.3 IMPLEMENTATION OF STATUTORY REQUIREMENTS ON AIR EMISSION MANAGEMENT

This activity requires to:

- Verify, in connection with applicable legislation, the need to obtain an air-emission authorization for the entire site;
- Obtain the authorization by the time limits in applicable legislation and implement controls required by applicable legislation in plants that have not been authorized yet;
- Implement requirements in authorizations on: collection and conveyance method (emissions that are technically conveyable), compliance with emission limit values and requirements, sampling methods, required periodic checks;
- Maintain and renew by the deadlines in applicable legislation any emission authorization;
- Periodically check the proper implementation of the above requirements.

20.6.4 IMPLEMENTATION OF STATUTORY REQUIREMENTS ON OZONE-DEPLETING SUBSTANCE MANAGEMENT

This activity requires to:

- Check the existence of any systems containing ozone-depleting substances, identifying any type of substance in use;
- Check that any ozone-depleting substances inside devices or plants are used in applications that are allowed by applicable legislation. If plants or devices contain prohibited ozone-depleting substances, specialized companies will have to replace them with authorized substances;
- Periodically have the monitoring specialist check if refrigeration systems and equipment and air-conditioning systems feature the presence of leaks in refrigeration circuits;
- Keep a system booklet that is consistent with the form set out in applicable legislation;
- The system booklet must list all recovery and recycle operations, time of inspections, outcome of inspections. Recovery operations of CFC or HCFC in the refrigerating circuit of refrigeration systems and equipment, air conditioning and heat pumps must be completed with certified devices;

- Check that the use of HCFC in fire protection systems and fire extinguishers is allowed by applicable legislation for those applications;
- Periodically check the proper implementation of the above requirements.

20.6.5 THE KILLING, DESTRUCTION, CATCHING, POSSESSION OR TAKING OF SPECIMENS OF PROTECTED WILD FAUNA OR FLORA SPECIES IN CONNECTION

In the case of leather-wear, documents on imports or purchase must be annexed to the supplier's statement as per regulations on the protection of animals (under: Art. 727-bis Criminal Code, Art. 733-bis Criminal Code – Law 150/1992, Art. 1, para. 1, Art. 2, para. 1 and para. 2, Art. 6, para. 4 – Law 150/1992, Art. 1, para. 2 – Law 150/1992, Art. 3-bis, para. 1 – EC Regulations 338/1997 and 939/1997).

20.6.6 ENVIRONMENTAL EMERGENCY MANAGEMENT

If anomalous events occur, including with no willful intent, capable of having significant impact on the environment with significant and measurable damages or deterioration of water or air, or an extensive or significant portion of soil or subsoil (water cycle, waste cycle, air emissions, etc.), the procedure for emergency management, including environmental emergencies, will have to be followed in detail.

20.6.7 FORMALIZATION OF ROLES AND REMIT, AND RELATED MANAGEMENT RESPONSIBILITIES

This activity requires to:

- Prepare and maintain a corporate organization appropriate to oversee the risks of committing environmental offenses;
- Formalize the Company organization, with the specific indication of functions and duties assigned, through appropriate instruments and powers of attorney.

20.6.8 APPROPRIATE INFORMATION AND TRAINING OF WORKERS

This activity requires to:

- Arrange information sessions for all workers;
- Arrange information and training of workers who are staffed to operations featuring a high risk of an offense being committed within the corporate organization;
- Arrange information sessions for workers of external companies that operate on the sites of CONBIPEL.

20.6.9 SUPERVISION ON COMPLIANCE WITH ENVIRONMENTAL PROCEDURES AND INSTRUCTIONS

This activity requires to:

- Arrange an appropriate supervision system on workers' compliance with environmental safety procedures and measures, identifying specifically delegated persons within a Production Unit;

- Arrange internal environmental protection and safety regulations appropriate for environmental risks.

20.6.10 OBTAINING AUTHORIZATIONS AND CERTIFICATIONS REQUIRED BY THE LAW

This activity requires to:

- Acquire and keep record of documents concerning requirements in applicable environmental legislation, regulations and provisions;
- Keep documents relating to authorization procedures, authorizations, certifications and any relevant documents, as well as any documents containing addendums or changes;
- Keep documents relating to internal corporate regulations.

20.6.11 PERIODIC INTERNAL CHECKS ON THE APPLICATION AND EFFECTIVENESS OF ADOPTED PROCEDURES

This activity requires to:

- Check and possibly supplement internal procedures for the prevention of environmental offenses, consistently with the specific nature of risks of breaches of provisions in Art. 25-*undecies* of Leg. Dec. No. 231/2001, considering all operations completed in the management of environmental protection, harmonizing them also for the purpose of compliance with Leg. Dec. 231/2001, preventing useless and costly duplications;
- Constantly monitor corporate procedures, ensuring their appropriate and timely revision, especially in the event of:
    - any increase in the level of risk;
    - emergency;
    - significant changes in environmental protection regulations;
    - changes in the Company's organization;
    - significant changes for the introduction of new technologies.

20.6.12 APPROPRIATE CONTROL SYSTEMS ON MAINTAINING IN TIME APPROPRIATE CONDITIONS OF ADOPTED ENVIRONMENTAL MEASURES AND RECORD KEEPING OF COMPLETION OF THE ACTIVITIES LISTED ABOVE

This activity requires to:

- Monitor environmental regulations and their requirements;
- Periodically check compliance with administrative requirements set out in environmental legislation with reference to the previous semester;
- Ensure that paper or IT records of Six-month audit reports on compliance with conventional environmental legislation for sites, are kept and updated, for the purpose of the checks referred to above.

20.7 TRACEABILITY

Appropriate record of all requirements in this policy must be kept by the persons responsible for them.

Traceability is also guaranteed by filing electronically any process documents.

All documents are recorded by the parties responsible for them and are filed in the area of the Company to which they belong[33].

[33] "Document management" procedure.

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION M
Transnational Crime

21. TRANSNATIONAL CRIME

21.1 CASES OF TRANSNATIONAL CRIME (ART. 10 LAW NO. 146 DATED 16.3.2006)

This Special Section concerns Transnational Crime (Art. 10 Law. no. 146 of 16.3.2006).

Individual offenses are described in Art. 10, Law No. 146 of 16.3.2006 (see ANNEX 1: catalog of predicate offenses).

21.2 SENSITIVE PROCESSES IN THE AREA OF TRANSNATIONAL CRIME

The following sensitive processes emerged in connection with transnational crime:

- Purchase and/or sale agreements entered into with foreign companies;
- Managing cash flows with foreign companies.

Activities were detected in each process.

Involved company roles:

- CEO;
- CFO, Treasury Manager, Financial Control, Accounting & Administration Manager, Import Manager;
- Commercial Director, Retail Managers, Real Estate Manager, Business Operation Control Manager;
- Product Director, Product Managers, Technical Services Manager, Sourcing Manager;
- Logistic Manager.

21.3 GENERAL CONDUCT PRINCIPLES

The following general prohibitions apply directly to Corporate Bodies, Executives and Employees, while they apply to Consultants, Suppliers and Partners in view of specific contract clauses.

The above parties are prohibited from adopting, participating in or causing the adoption of conducts that, individually or collectively, qualify as the offenses referred to above. Breaches of corporate principles and procedures in this Special Section are also prohibited.

Consistently with the Code of Ethics, corporate procedures, policies and regulations, requirements applicable to the parties identified include but are not limited to:

- Refraining from adopting, cooperating in or causing the adoption of conducts qualifying as cases of transnational crime;

- All operations and transactions carried out on behalf of CONBIPEL S.p.A. – including in intercompany relations with foreign companies – must be inspired by utmost compliance with applicable laws and regulations and the principles of fairness, transparency, good faith and traceability of documents;
- The principle of segregation of roles and responsibilities in the various phases of corporate processes must be complied with;
- Compliance with applicable legislation and corporate procedures and policies is guaranteed, including with respect to completion of the necessary reviews on foreign assets and resources, including prior reviews;
- Actual conducts and conducts required by internal procedures must be absolutely in line.

21.4 SPECIFIC PROCEDURAL PRINCIPLES

To supplement and give operating details on the principles stated in the Code of Ethics, specific polices were defined (*treasury/financial resources management policy, policy on the procurement of goods, services, consulting, professional services*) that, in addition to clearly defining roles and responsibilities of players involved in the process, set out a number of specific and material controls to mitigate risk factors, and namely require that business and financial transactions with foreign companies of the Group must:

- Be approved in compliance with specific powers to authorize granted within the Company;
- Be periodically reconciled in the manner and times set out in specific procedures.

Moreover, the following additional policies must be complied with:

- Settled financially based on corporate regulations on transactions with controlled companies in compliance with applicable legislation and provisions having the force of a contract applicable to all controlled companies;
- Check that the quality and quantity of products stated in the transport document of purchased goods match the purchase order;
- Make formal and substantial checks on all imported materials;
- Arrange checks for the accounting reconciliation of amounts paid and received products, and the inventory reconciliation of goods ordered and goods on stock;
- Approve purchase orders for direct capital goods on the Company's IT system based on defined authorization levels;
- Formalize relations with intercompany suppliers by entering into framework agreements / contracts / letters of engagement which include the clause on compliance with the Model and Code of Ethics, with a view to punishing any conducts/behaviors that are contrary to ethical principles;
- Give documentary proof of the suppliers' selection and approval process by an appropriate hierarchical level (based on the amount of the purchase).

Organization, management and control Model under Leg. Dec. 231/2001

SPECIAL SECTION N
Offenses Related to Immigration

22. OFFENSES RELATED TO IMMIGRATION

22.1 CASES OF OFFENSES RELATED TO IMMIGRATION

This Special Section refers to the offenses of Employment of illegally staying third-country nationals, Causing illegal entry and Abetting illegal stay.

Individual cases are described in Art. 25 *duodecies* of Leg. Dec. 231/2001 (see ANNEX 1: catalog of predicate offenses).

22.2 SENSITIVE PROCESSES IN THE AREA OF OFFENSES RELATED TO IMMIGRATION

In connection with offenses and criminal conducts in the area of offenses related to immigration, the following areas feature risks:

i. entrusting engagements for works and services: this involves the management of the choice and engagement of self-employed contractors for works or services that they undertake to render personally, "independently" and with no "bond of subordination", and therefore not under a subordinate employment arrangement;

ii. hiring subordinate employees.

Involved company roles:

- CEO;
- Human Resources Manager;
- Commercial Director, Retail Managers;
- Product Director, Product Managers, Technical Services Manager, Sourcing Manager;
- Logistic Manager.

22.3 GENERAL PRINCIPLES OF CONDUCT

22.3.1 GENERAL PRINCIPLES

The following general principles apply to Addressees, or all parties to the extent that they are involved in performing activities that are included in risk-featuring areas and in consideration of their different positions or obligations with the Company.

Specifically, this Special Section intends to:

a) provide a list of general principles and specific procedural principles which Addressees must comply with to correctly apply the Model;

b) give the SC and corporate function managers called to cooperate with it the principles and operating tools necessary to exercise its control, monitoring and audit activities.

In performing their activities/functions, in addition to the rules in this Model, company officers are required, in general to comply with all rules and principles contained in the following documents, in the sections that pertain to them:

1. Organization chart and organization tables
2. HR Management Procedure
3. General terms of purchase.

22.3.2 GENERAL PRINCIPLES OF CONDUCT AND SPECIFIC PREVENTION POLICIES

This Special Section expressly prohibits to:

- Adopt conducts cable of qualifying as the above offenses (under Art. 25-*duodecies* of the Decree) or conducts which, albeit alone are not offenses, may qualify as of the ones under review herein;
- Breach the principles and procedures existing in the Company on hiring foreign employees and/or in this Special Section.

Accordingly, this Special Section expressly requires the above parties to:

- Adopt a proper, transparent and cooperative conduct, in compliance with legislation on the employment of third country nationals;
- Deliver, without delay, correctly and in good faith, all notices required by laws and regulations to supervisory authorities, without interfering howsoever with any supervisory activities performed by them;
- Arrange the necessary training and information sessions.

Moreover, specific prevention Policies regulate individual sensitive activities, in whose scope some of the offenses related to immigration could potentially be committed.

a) For transactions concerning Engagements for works or services, in addition to compliance with the policies in paragraph 18.3, the Company sets:
    - A specific procedure/checklist to execute agency work agreements, services and works contracts;
    - An appropriate system of delegations of powers and powers of attorney for the execution of agreements that require the use of labor by the other party to such agreement;
    - Authorization procedures for purchases;
    - Specific requests for suppliers or business partners to expressly commit to the provisions under review.

b) When hiring subordinate employees, in addition to the procedures in paragraph 11.6, the following policies need to be followed:

- Make the prior checks acquiring prior information including from the relevant authorities that third-country nationals that are candidates for employment have valid residence permit documents and meet general conditions for employment;
- Make subsequent checks that residence permit documents of third-country nationals employed by the Company remain valid.