INDUSTRIE DE NORA S.P.A.

Organisation,
Management and Control Model
pursuant to Italian Legislative Decree no. 231/2001

Document	**Organisation, Management and Control Model**

Approval	Board of Directors	minutes dated	05.05.2021
Revision	**no. 5**	Supervisory Body verification of	05.05.2021
Previous Versions	no. 4 no. 3 no. 2 no. 1	Board of Directors minutes dated	30.05.2018 12.09.2016 21.05.2014 20.12.2012

Signatures of the Supervisory Body			
Signature for the Board of Directors Chief executive Officer			

CONTENTS

GENERAL SECTION

CHAPTER 1
CORPORATE LIABILITY REGIME **10**

INTRODUCTION: THE REGULATORY SYSTEM UNDER LEGISLATIVE DECREE No. 231/2001 10

IMPLEMENTATION OF LEGISLATIVE DECREE No. 231/2001 14

RECIPIENTS OF THE MODEL 15

ORGANISATION AND MANAGEMENT MODEL 15
- Purpose and objectives of the Model
- Structure of the Model

ADOPTION OF THE MODEL 16
- Approval of the Model
- Amendments and additions

CHAPTER 2
THE CRIME RISK CONTROL SYSTEM

INTRODUCTION: COMPANY CONTEXT 17
- The company's governance structure

GENERAL PRINCIPLES OF CONTROL 18
- Integrated organisational structure documentation
- System of Delegations
- Integrated internal regulatory system
- Risk mapping

SUPERVISORY BODY (SB) 20
- Identification of the SB
- SB prerogatives and resources
- SB functions and powers

INTERNAL INFORMATION FLOWS 21

- Reporting obligations to the SB
- Whistleblowing Regulations (Italian Law No. 179 of 30.11.2017)
- SB activities consequent to the report
- Relationships between the SB and the corporate bodies
- Relationships between the SB and the Board of Statutory Auditors
- Relationships between the IDN SB and the DNIT and DNWT SBs
- Relationships between the SB and other entities

DISCIPLINARY SYSTEM 28
- General principles
- Sanctions against the Directors
- Sanctions against the Sole Auditor
- Sanctions against employees
- Measures against external collaborators

DISSEMINATION AND AWARENESS OF THE MODEL 29
- Staff training
- Information for external collaborators

PERIODIC CHECKS 31

* * *

SPECIAL SECTION

CHAPTER 3
CORPORATE CRIMES 33

RISK AREAS 35

RECIPIENTS OF THE SPECIAL SECTION 36

GENERAL CODE OF CONDUCT 36

SPECIAL CODE OF CONDUCT 36
- Communications to the shareholders and to third parties

- Management of Relationships with the Board of Statutory Auditors
- Protection of share capital
- Management of intercompany relationships
- Corruption among private entities

DUTIES OF THE SB 40

CHAPTER 4
CRIMES AGAINST PUBLIC ADMINISTRATION 41

RECIPIENTS OF THE SPECIAL SECTION 43

RISK AREAS 44

CONTROL MEASURES 44

CODE OF CONDUCT 44

DUTIES OF THE SB 46

CHAPTER 5
CRIMES IN RELATION TO WORKPLACE SAFETY 47

RISK AREAS 50

RECIPIENTS OF THE SPECIAL SECTION 53

CODE OF CONDUCT 53
- General code of conduct
- Code of Conduct: relationships with contractors
- Risks from hazardous chemical substances
- Fire risks
- Risks from biological agents

DUTIES OF THE SB 57

CHAPTER 6
CYBER CRIMES 59

RISK AREAS 62

RECIPIENTS OF THE SPECIAL SECTION 63

CODE OF CONDUCT 63

DUTIES OF THE SB 64

CHAPTER 7
CRIMES AGAINST TRADE AND INDUSTRY 66

RISK AREAS 69

RECIPIENTS OF THE SPECIAL SECTION 69

CODE OF CONDUCT 69

DUTIES OF THE SB 70

CHAPTER 8
CRIMES OF RECEIVING, LAUNDERING AND USING MONEY AND GOODS OF ILLEGAL ORIGIN AND SELF-LAUNDERING 72

RISK AREAS 73

RECIPIENTS OF THE SPECIAL SECTION 74

CODE OF CONDUCT 75

DUTIES OF THE SB 76

CHAPTER 9
CRIMES IN RELATION TO THE ENVIRONMENT 77

RISK AREAS 82

RECIPIENTS OF THE SPECIAL SECTION 82

CODE OF CONDUCT 83

DUTIES OF THE SB 84

CHAPTER 10
INCITEMENT NOT TO TESTIFY OR TO BEAR FALSE WITNESS 85

RISK AREAS 85

RECIPIENTS OF THE SPECIAL SECTION 85

CODE OF CONDUCT 85

DUTIES OF THE SB 86

CHAPTER 11
CRIMES IN RELATION TO ILLEGAL IMMIGRATION 87

RISK AREAS 88

RECIPIENTS OF THE SPECIAL SECTION 88

CODE OF CONDUCT 88

DUTIES OF THE SB 88

CHAPTER 12
ORGANISED CRIMES, DOMESTIC AND TRANSNATIONAL 89

RISK AREAS 89

RECIPIENTS OF THE SPECIAL SECTION 90

CODE OF CONDUCT 90

DUTIES OF THE SB 91

CHAPTER 13
CRIMES IN RELATION TO INFRINGEMENT OF COPYRIGHT 92

RISK AREAS 92

RECIPIENTS OF THE SPECIAL SECTION 92

CODE OF CONDUCT 92

DUTIES OF THE SB 93

CHAPTER 14
CRIMES AGAINST THE INDIVIDUAL 94

RISK AREAS 94

RECIPIENTS OF THE SPECIAL SECTION 95

CODE OF CONDUCT 95

DUTIES OF THE SB 96

CHAPTER 15
CRIMES IN RELATION TO RACISM AND XENOPHOBIA 97

RISK AREAS 97

RECIPIENTS OF THE SPECIAL SECTION 97

CODE OF CONDUCT 97

DUTIES OF THE SB 98

CHAPTER 16
TAX CRIMES 99

RISK AREAS 101

RECIPIENTS OF THE SPECIAL SECTION 101

CODE OF CONDUCT 102
- Management of tax obligations
- Sales and distribution cycle and purchasing cycle
- Management of receipts and payments
- Management of intercompany relationships

DUTIES OF THE SB 105

CHAPTER 17
CRIMES OF MARKET ABUSE 106

RISK AREAS 106

CODE OF CONDUCT, PROCEDURES AND CONTROL MEASURES 106
- Management of external communications

DUTIES OF THE SB 108

* * *

ANNEXES

- Organisation Chart
- Group Code of Ethics
- Disciplinary System
- Regulatory Appendix

GENERAL SECTION

CHAPTER 1

CORPORATE LIABILITY REGIME

INTRODUCTION: THE REGULATORY SYSTEM UNDER LEGISLATIVE DECREE NO. 231/2001

With the approval of Italian Legislative Decree no. 231 of 8 June 2001 (hereinafter, for simplicity, the Decree), entitled "*Rules on corporate liability of legal persons, companies and associations, also without legal status*" a complex and innovative sanction system was introduced into the Italian legal framework, identifying forms of liability of an administrative nature for Entities as a[1] consequence of the commission of a number of crimes. This is on the condition that the crime is implemented in the interest or to the advantage of the Entity itself and that the perpetrators of said crime are:

1) persons who, in the Entity's organisational structure, cover a "senior" position (namely, in accordance with Art. 5, paragraph 1, "*persons who cover roles of representation, administration or management of the entity or of one of its organisational units having financial and functional autonomy, as well as persons who exercise, also de facto, management and control of the same*");
2) "*persons subject to management or supervision*" of the latter.

This concerns liability that the legislator defines as "administrative" but which, in actual fact, has strong similarities to criminal liability. In fact, it arises by virtue of and as a consequence of the commission of a crime (and not an administrative offence); it is ascertained in criminal proceedings; the sanction measure is always a jurisdictional act (for example: a judgement); and, above all, it is autonomous with respect to the liability of the natural person who committed the crime. Hence, in accordance with Art. 8 of the Decree, the Entity may be declared liable even if the natural person who committed the crime cannot be indicted, has not been identified, or if the crime has expired for a reason other than a formal pardon.

In order for the Entity's liability to exist, the crime committed must be attributable to it on a material level and must also constitute the manifestation of an express will or at least derive from the fault of the organisation, thereby meaning a failure to adopt the necessary controls to avoid the commission of the crime itself or the adoption of insufficient controls.

Vice versa, the Entity's liability is expressly excluded if the perpetrator of the violation acted in his/her exclusive interest or that of third parties.

At the date of drawing up this Model, the crimes susceptible to determining corporate liability are the following:

- **crimes against public administration**: misuse of money to the detriment of the State (Art. 316-bis of the Italian Criminal Code); undue receipt of payments to the detriment of the State (Art. 316-ter of the Italian Criminal Code); fraud to the detriment of the State or another public entity or the European Union (Art. 640, paragraph 2 of the Italian Criminal Code); aggravated fraud to

[1] In accordance with Italian Legislative Decree 231/2001, "Entities" are intended as:
- entities having legal personality, such as joint stock companies, limited liability companies, partnerships limited by shares, cooperatives, recognised associations, foundations, other financial public and private entities;
- entities not having legal personality, such as general partnerships, limited partnerships, also irregular, unrecognised associations.

obtain public funds (Art. 640-bis of the Italian Criminal Code); cyber fraud (640 ter of the Italian Criminal Code); corruption in carrying out duties or through actions contrary to official duties (Articles 318, 319, 319 bis and 321 of the Italian Criminal Code); corruption of a public official (Art. 320 of the Italian Criminal Code); corruption in judicial deeds (Art. 319-ter of the Italian Criminal Code); undue incitement to give or promise gains (Art. 319-quater of the Italian Criminal Code); incitement to corruption (Art. 322 of the Italian Criminal Code); extortion (Art. 317 of the Italian Criminal Code); embezzlement, extortion, undue incitement to give or promise gains, corruption and incitement to corruption of members of the International Criminal Court or bodies of the European Communities and officials of the European Communities and foreign countries (Art. 322-bis of the Italian Criminal Code), influence peddling (Art. 346-bis of the Italian Criminal Code); abuse of office (Art. 323 of the Italian Criminal Code); [2]

- **cyber crimes and illegal data processing**: falsification of electronic documents (Art. 491-bis of the Italian Criminal Code); illegal access to a computer or electronic system (Art. 615-ter of the Italian Criminal Code); illegal possession and dissemination of access codes to computer or electronic systems (Art. 615-quater of the Italian Criminal Code); dissemination of equipment, devices or computer programmes aimed at damaging or interrupting a computer or electronic system (Art. 615-quinquies of the Italian Criminal Code); interception, impediment or illegal interruption of computer or electronic communications (Art. 617-quater of the Italian Criminal Code); installation of interception devices; impeding or interrupting computer or electronic communications (Art. 67-quinquies of the Italian Criminal Code); damage of information, data and computer programmes (Art. 635-bis of the Italian Criminal Code); damage of information, data and IT programmes used by the State or by another public entity or in any case of public interest (Art. 635-ter of the Italian Criminal Code); damage of computer or electronic systems (Art. 635-quater of the Italian Criminal Code); damage of computer and electronic systems of public interest (Art. 635-quinquies of the Italian Criminal Code)[3];
- **organised crimes**: conspiracy (Art. 416 of the Italian Criminal Code); Mafia-like conspiracy, domestic or foreign (Art. 416-bis of the Italian Criminal Code)[4];
- **crimes against the public trust**: counterfeit of currency, complicit spending and introduction into the country of counterfeit currency (Art. 453 of the Italian Criminal Code); alteration of currency (Art. 454 of the Italian Criminal Code); non-complicit spending and introduction into the country of counterfeit currency (Art. 455 of the Italian Criminal Code); spending of counterfeit currency received in good faith (Art. 457 of the Italian Criminal Code); falsification of revenue stamps, introduction into the country, purchase, possession or placement in circulation of falsified revenue stamps (Art. 459 of the Italian Criminal Code); counterfeiting, alteration or use of trademarks or logos or patents, models and designs (Art. 473 of the Italian Criminal Code); introduction into the country and trade of products with false markings (Art. 474 of the Italian Criminal Code)[5]
- **crimes against trade and industry**: disruption of the freedom of trade and industry (Art. 513 of the Italian Criminal Code); unfair competition with threats or violence (Art. 513-bis of the Italian Criminal Code); fraud against national industries (Art. 514 of the Italian Criminal Code); fraud in the exercise of trade (Art. 515 of the Italian Criminal Code); sale of non-genuine

[2] Cf. Articles 24 and 25, Italian Legislative Decree no. 231/2001.
[3] Cf. Art. 24-bis of Italian Legislative Decree no. 231/2001, inserted by Art. 7 of Italian Law no. 48 of 18.03.2008.
[4] Cf. Art. 24-ter of Italian Legislative Decree no. 231/2001, inserted by Art. 2, paragraph 29 of Italian Law no. 94 of 15.07.2009
[5] Cf. Art. 25-bis of Italian Legislative Decree no. 231/2001, as amended most recently by Italian Law no. 99 of 23.07.2009

foodstuffs as genuine (Art. 516 of the Italian Criminal Code); sale of industrial products with false markings (Art. 517 of the Italian Criminal Code); manufacture and trade of goods created usurping industrial property rights (Art. 517-ter of the Italian Criminal Code); counterfeiting of geographical indications or designations of origin of agri-food products (Art. 517-quater of the Italian Criminal Code);[6]

- **corporate crimes**: false corporate communications (Art. 2621 and Art. 2622 of the Italian Civil Code); impeded control (Art. 2625 of the Italian Civil Code); fictitious formation of capital (Art. 2632 of the Italian Civil Code); undue return of contributions (Art. 2626 of the Italian Civil Code); illegal allocation of profits and reserves (Art. 2627 of the Italian Civil Code); illegal transactions on company stocks or shares or those of the parent company (Art. 2628 of the Italian Civil Code); transactions prejudicial to creditors (Art. 2629 of the Italian Civil Code); undue allocation of company assets by liquidators (Art. 2633 of the Italian Civil Code); corruption among private entities (Art. 2635 of the Italian Civil Code); incitement to corruption among private entities (Art. 2635-bis of the Italian Criminal Code); unlawful influence on the shareholders' meeting (Art. 2636 of the Italian Civil Code);[7]
- **crimes against the individual**: illegal intermediation and exploitation of labour (Art. 603-bis of the Italian Criminal Code);[8]
- **crimes in relation to workplace safety**: manslaughter (Art. 589 of the Italian Criminal Code); actual or grievous bodily harm (Art. 590, second paragraph of the Italian Criminal Code), if committed in violation of the rules on workplace health and safety;[9]
- **crimes in relation to receiving, laundering and self-laundering**: receiving (Art. 648 of the Italian Criminal Code); laundering (Art. 648-bis of the Italian Criminal Code); reuse of money, goods or gains of illegal origin (Art. 648-ter); self-laundering (Art. 648-ter1 of the Italian Criminal Code)[10];
- **crimes in relation to infringement of copyright**: envisaged respectively by Articles 171, 171-bis, 171-ter, 171-septies and 171-octies of Italian Law no. 633 of 22.04.1941[11];
- **crimes of incitement to not testify or to bear false witness before judicial authorities**: Art. 377-bis of the Italian Criminal Code[12];
- **environmental crimes:** environmental pollution (Art. 452-bis of the Italian Criminal Code); environmental disaster (Art. 452-quater of the Italian Criminal Code); unintentional crimes against the environment (Art. 452-quinquies of the Italian Criminal Code); conspiracy for the purpose of committing environmental crimes (Art. 452-octies of the Italian Criminal Code); unauthorised waste management activity (Art. 256 of Italian Legislative Decree 152/2006); failure to reclaim sites (Art. 257 of Italian Legislative Decree 152/2006); violation of obligations to communicate

[6] Cf. Art. 25-bis 1 of Italian Legislative Decree no. 231/2001, inserted by Art. 15, paragraph 7, letter b) of Italian Law no. 99 of 23.07.2009

[7] See Art. 25-ter of Italian Legislative Decree no. 231/2001, as amended most recently by Art. 6, paragraph 1 of Italian Legislative Decree no. 38 of 15.03.2017

[8] Cf. Art. 25-quinquies of Italian Legislative Decree 231/2001, as amended most recently by Art. 6, paragraph 1 of Italian Law no. 199 of 29.10.2016.

[9] Cf. Art. 25-septies of Italian Legislative Decree 231/2001, as amended most recently by Art. 300 of Italian Legislative Decree no. 81 of 9.04.2008

[10] Cf. Art. 25-octies of Italian Legislative Decree 231/2001, as amended most recently by Art. 5 of Italian Legislative Decree no. 90 of 25.05.2017

[11] Cf. Art. 25-nonies of Italian Legislative Decree 231/2001, inserted by Art. 15, paragraph 7 of Italian Law no. 99 of 23.07.2009.

[12] Cf. Art. 25-decies of Italian Legislative Decree 231/2001, inserted by Art. 4 of Italian Law no. 116 of 3.08.2009

and keep mandatory records and forms (Art. 258 of Italian Legislative Decree 152/2006); illegal waste trafficking (Art. 259 of Italian Legislative Decree 152/2006); organised activities for the illegal trafficking of waste (Art. 260 of Italian Legislative Decree 152/2006); rules in relation to protection of the air and reduction of atmospheric emissions - sanctions (Art. 279 of Italian Legislative Decree 152/2006)[13]**;**

- **crimes in relation to illegal immigration**: Art. 12, paragraph 3 and Art. 22, paragraph 12-bis of Italian Legislative Decree no. 286 of 25.07.1998[14],
- **crimes relating to racism and xenophobia**: Art. 3, paragraph 3-bis of Italian Law No. 654 of 13.10.1975.
- **tax crimes:** fraudulent misrepresentation using invoices or other documents for non-existent transactions (Art. 2 of Italian Legislative Decree no. 74/2000); fraudulent misrepresentation by means of other deception (Art. 3 of Italian Legislative Decree no. 74/2000); issuance of invoices or other documents for non-existent transactions (Art. 8 of Italian Legislative Decree no. 74/2000); concealment or destruction of accounting documents (Art. 10 of Italian Legislative Decree no. 74/2000); fraudulent evasion of tax payments (Art. 11 of Italian Legislative Decree no. 74/2000); false statement in a tax return (Art. 4 of Italian Legislative Decree no. 74/2000); failure to file a tax return (Art. 5 of Italian Legislative Decree no. 74/2000); illegal offsetting in a tax return (Art. 10-quater of Italian Legislative Decree no. 74/2000)[15].
- **smuggling:** smuggling in the movement of goods across land borders and customs areas (Art. 282 of Italian Presidential Decree no. 73/1934); smuggling in the movement of goods in border lakes (Art. 283 Italian Presidential Decree no. 73/1943); smuggling in the maritime movement of goods (Art. 248 Italian Presidential Decree no. 73/1943); smuggling in the movement of goods by air (Art. 285 Italian Presidential Decree no. 73/1943); smuggling in non-customs areas (Art. 286 Italian Presidential Decree no. 73/1943); smuggling for undue use of goods imported with customs duty concessions (Art. 287 Italian Presidential Decree no. 73/1943); smuggling in customs deposits (Art. 288 Italian Presidential Decree no. 73/1943); smuggling in cabotage and in circulation (Art. 290 Italian Presidential Decree no. 73/1943); smuggling in the export of goods eligible for return of duties (Art. 290 Italian Presidential Decree no. 73/1943); smuggling in temporary import or export (Art. 291 Italian Presidential Decree no. 73/1943); smuggling of foreign produced tobacco (Art. 291-bis Italian Presidential Decree no. 73/1943); criminal conspiracy to smuggle foreign produced tobacco (Art. 291-ter Italian Presidential Decree no. 73/1943); criminal conspiracy to smuggle tobacco (Art. 291-quater Italian Presidential Decree no. 73/1943); other cases of smuggling (Art. 292 Italian Presidential Decree no. 73/1943); criminal conspiracy to smuggle (Art. 295 Italian Presidential Decree no. 73/1943).[16]

The list of crimes indicated in Art. 24 et seq. of the Decree is not to be considered definitive and may be subsequently modified, also based upon the continuous alignment of domestic legislation with international legislation and, in this case, EU legislation.

[13] Cf. Art. 25-undecies of Italian Legislative Decree 231/2001, as amended most recently by Art. 1 of Italian Law no. 68 of 22.05.2015

[14] Cf. Art. 25-duodecies of Italian Legislative Decree 231/2001, as amended most recently by Art. 39, paragraph 4 of Italian Law no. 161 of 17.10.2017.

[15] Cf. Art. 25-quinquiesdecies of Italian Legislative Decree 231/2001, inserted by Law no. 157/2019.

[16] Cf. Art. 25-sexiesdecies of Italian Legislative Decree 231/2001, inserted by Italian Law no. 75/2020; at present, these types of crime are considered to have little impact on the company situation.

The sanctions envisaged for cases in which the Entity's liability is ascertained are particularly rigorous. Financial penalties and/or bans are applied (the latter identified by Art. 9 of the Decree as a ban from exercising the activity, suspension or revocation of authorisations functional to the commission of the crime, prohibition on contracting with Public Administration, exclusion from subsidies, funding, contributions or grants with the possibility of revoking those already granted and a ban on advertising goods or services), as well as confiscation of the price or profit of the crime and publication of the conviction ruling.

The financial penalty is determined by the criminal court through a system based upon "shares" in an amount not less than one hundred and not more than one thousand (the amount of each share may vary from a minimum of €258 to a maximum of €1,549). Conversely, the court determines the type and duration of the ban taking account of the suitability of the individual penalties to prevent crimes of the nature of that which was committed and, if necessary, may apply them jointly.

The sanctions (financial penalties and bans) may also apply, albeit in reduced form (with regard to their amount and duration), in relation to the commission of crimes in the form of an attempt, except where the Entity has voluntarily prevented the completion of the action or implementation of the act: in such cases, the Entity may be immune from any consequence.

During the criminal proceedings, the judge may then order, by the methods envisaged by the code of criminal procedure, the seizure of the price or profit of the crime for confiscation, which - at the end of the case - will be applied with the conviction ruling against the Entity itself. Furthermore, if there are grounds to consider that the guarantees for payment of the financial penalty, the costs of the proceedings and any other sum due to the State are absent or have dissipated, the Public Prosecutor may request - at any stage and level of the trial - the conservative seizure of the moveable and/or immovable assets of the Entity or the sums or items due to it.

The liability envisaged by the Decree also exists in relation to crimes committed abroad, provided that the country in which the crime was committed does not prosecute such crimes.

Corporate liability, for which the indicated sanctions may be applied, is therefore based upon "organisational" fault: in other words, the Entity is considered liable for the crime committed by its representative if it failed to establish an organisation able to effectively prevent its implementation and, in particular, if it failed to equip itself with an internal control system and adequate procedures for controlling the correct conduct of the activities at most risk of commission of the crimes.

In the face of such a strict penalty system, however, Art. 6 paragraph 1 of the Decree excludes the Entity's liability if, inter alia, it has adopted and effectively implemented, prior to the commission of the act, organisation and management models suitable to prevent crimes of the nature of that which occurred and it has also entrusted to a Body within the Entity, having autonomous powers of initiative and control, the duty to oversee the functioning and observance of the models and to deal with their periodic update.

In accordance with the provisions of Art. 6, paragraph 2 of the Decree, the Model must, in particular, meet the following requirements:

1. identify the activities in the field of which the crimes may be committed;

2. envisage specific protocols to plan the formation and implementation of the Entity's decisions in relation to the crimes to be prevented;
3. identify methods of managing financial resources suitable to prevent the commission of the crimes;
4. envisage reporting obligations to the Body in charge of overseeing the functioning and compliance with the models;
5. introduce a disciplinary system suitable to sanction any failure to comply with measures specified by the Model.

These models, as envisaged by Art. 6, paragraph 3 of the Decree, may also be adopted based upon codes of conduct prepared by trade associations representing the Entities.

IMPLEMENTATION OF LEGISLATIVE DECREE No. 231/2001

Although the Decree does not envisage the mandatory implementation of the Model, in order to avoid as much as possible any unlawful act by persons occupying a "senior" position as well as by its employees, Industrie De Nora Italy s.r.l. (hereafter, the "Company" or "IDN"), has adopted a specific Model, duly approved by the Board of Directors by resolution dated 20.12.2012.

Updated versions of this Model were approved subsequently by resolution of 21.05.2014 (Revision 2), resolution of 12.09.2016 (Revision 3) and resolution of 30.05.2018 (Revision 4), respectively. The current version is therefore no. 5.

As part of the implementation of provisions of the Decree, the Board of Directors, in putting the Model into effect, has entrusted the role of internal control body to a Supervisory Body (hereinafter, for simplicity, SB), having autonomous duties of supervision, control and initiative in relation to the Model itself.

The SB is responsible for ensuring that the Entity has a suitable organisational model and overseeing its effective implementation, ascertaining the effectiveness of its functions and ensuring it is progressively updated, so as to guarantee constant adjustment to subsequent changes of an operational and/or organisational nature.

RECIPIENTS OF THE MODEL

The recipients of the rules and requirements contained in the Model comprise all Company representatives: shareholders, directors, members of the other corporate bodies, and employees.

The following are also recipients of the Model and are thus required to respect its contents: external collaborators, freelancers, consultants as well as any commercial and/or industrial partners.

ORGANISATION AND MANAGEMENT MODEL

Articles 6 and 7 of the Decree regulate cases in which the Entity is not liable for the crime committed by the persons indicated in Art. 5. These rules highlight a difference in terms of the regulation, and evidentiary laws governing crimes committed by persons in a senior position and those committed by subordinates.

In fact, by introducing a reversal of the burden of proof, Art. 6 envisages that the Entity is not liable for crimes committed by senior officers, if it demonstrates that:

1. the management body has adopted and effectively implemented, prior to the commission of the act, organisation and management models suitable to prevent crimes of the nature of that which occurred;
2. the duty to oversee the functioning and compliance with the models, as well as to deal with their relevant updates, has been entrusted to a Body of the Entity having autonomous powers of initiative and control;
3. the persons committed the crime by fraudulently evading the organisation and management models;
4. there was no omitted or insufficient supervision by the Body indicated in paragraph 2.

According to Art. 7, for crimes committed by persons subject to the management of others, the Entity is liable, on the other hand, only if the commission of the crime was rendered possible by a failure to comply with management or supervision obligations (but, in such circumstance, the burden of proof lies with the prosecution). In any event, such obligations are assumed to be complied with if the Entity, prior to the commission of the crime, adopted and effectively implemented an organisation, management and control model suitable to prevent crimes of the nature of that which occurred.

Purpose and objectives of the Model

The objective of the Model is to implement a structured and consistent system of procedures and control activities (preventive and subsequent), aimed at effectively combating the risk of committing the crimes, by identifying the activities at risk and their necessary regulation.

Consequently, the rules contained in this Model are intended, on the one hand, to make the potential perpetrator of the crimes aware of their illegality and the unfavourable stance taken by the Company towards such conduct, even where the Company might benefit, and, on the other hand, to allow the Company itself to intervene promptly to prevent or impede the perpetration of such crimes, by virtue of systematic monitoring of the activities and processes at risk.

The objectives of the Model thus include that of raising the awareness of both senior roles and those subordinate to the management of others as to the significance of the legislation in question, making them aware that in the event of conduct not compliant with the provisions of the Model, rules and associated procedures, laws and applicable regulations, the same may incur penalties - according to the rules contained in this document - and, regardless of any personal criminal liability, the Company may also incur liability, in accordance with the Decree, with the consequent application of financial penalties and/or bans.

Structure of the Model

This Model consists of a “General Section" and several “Special Sections”, prepared in relation only to those crimes considered by the Decree that, following risk mapping activity, are deemed likely to apply to the company's activities.

With regard to the other predicate offences envisaged by the Decree, it is considered that IDN's activity does not present high risk profiles or aspects that may be construed as reasonably possible for a crime to be committed. The conduct concerned is in fact deemed objectively extraneous to the Company's normal activity and therefore the latter, in light of the analysis performed, has considered compliance with the

Group's Code of Ethics (in addition to the general principles present here) to be adequate as a preventive measure.

The Board of Directors - also as proposed by the SB - has the power to adopt specific resolutions to supplement the Model, inserting additional Special Sections relating to the types of crimes that, by virtue of any future regulatory interventions, may be inserted or in any case related to the area of application of Italian Legislative Decree 231/2001.

ADOPTION OF THE MODEL

Approval of the Model

The Model must be approved by resolution of the Company's Board of Directors.

Amendments and additions

This Model is a document issued by the management body, in compliance with the provisions of Art. 6, paragraph 1, letter a) of the Decree: any subsequent amendments and additions of a substantial nature to the Model may be made - if necessary at the proposal of the SB - only by the Board of Directors.

Power is therefore granted to the Chairman - as well as to each director - to report to the Board of Directors, every time he/she considers it appropriate or necessary for any changes to be made to the Model.

CHAPTER 2

THE CRIME RISK CONTROL SYSTEM

INTRODUCTION: COMPANY CONTEXT

Industrie De Nora S.p.A. (hereinafter, the "Company" or "IDN") is a company limited by shares established in Italy, the majority of whose share capital is held by the parent company Federico De Nora S.p.A.; it is the holding company of the De Nora Group, where the corporate structures and services are centralised.

The company controls and coordinates intellectual property and makes decisions regarding the approach to the markets and which product portfolio and production strategies are to be adopted. The following corporate functions, providing services to the various Group companies, are centralised at Industrie De Nora S.p.A.: Administration, Finance and Control, Legal, Information and Communications Technology, Marketing, Business Development and Product Management, Global Operations, Production Technologies, Global Procurement and Human Resources.

Through its subsidiaries, IDN has a direct or indirect presence in various countries other than Italy, including Germany, the United Kingdom, the United States, China, India, Brazil, Japan, Singapore, Dubai and Abu Dhabi. The IDN Group is composed of IDN and its subsidiaries.

The IDN Group is a leader in the design, production and supply of products, technologies and complete solutions for electrochemistry.

The IDN Group's business is divided into the following activities:

- the Electrode Technologies Business;
- the Water Technologies Business.

The Electrode Technologies Business has been the core business of the Group since its establishment, while the Water Technologies Business is the business area established following the acquisition of the Water Purification Companies

The Electrode Technologies Business is mainly based on the Production and Marketing of (i) electrodes (anodes and cathodes) for the production of gas and industrial products (chlorine, caustic soda and derivatives), for the production of non-ferrous metals (nickel, cobalt, copper) for surface galvanising processes for both decorative and functional purposes, for protecting metallic or reinforced concrete structures from corrosion; (ii) metal-based catalytic varnishes (*coatings* and catalysts) such as iridium, ruthenium, platinum, palladium and rhodium, the formulations of which differ depending on the application for which they are intended and (iii) electrolysers and their components (separators and other cell components and accessories).
As part of the project to streamline and simplify the corporate structure of the Group, the Company transferred to its subsidiary De Nora Italy s.r.l. (hereinafter also referred to as "DNIT"), effective from 1 January 2018, the industrial activities in the sector of design, construction and marketing of electrodes, electrolysers for electrochemical plants and electrochemical systems for the production of biocides carried out at the Cologno Monzese (MI) plant, as well as at the Milan facility and the Singapore facilities.

The research and development activities in the electrochemical sector were not transferred and remain the activities of IDN which, in this field, retains a significant portfolio of trademarks and patents. However, the subsidiary DNIT is responsible for the production and commercial organisation of the industrial activities, including assets instrumental to the performance of those activities, the warehouse and a number of employment relationships.

All Italian and foreign companies controlled by IDN adopt the "De Nora" Code of Ethics, and the internal procedures ensure that, in managing the activities at risk for the purposes of corporate liability, all subsidiaries adopt principles and control measures coherent with the principles and control measures established by the Parent Company. In this regard, it should be noted that IDN has established an Ethics Committee which has the task of promoting the dissemination and implementation of the principles of the Code of Ethics in all Group companies, to carry out investigations in the event of reports, as well as to verify the adequacy of the Code of Ethics itself, incentivising any updates and additions.
The Company has its registered and administrative offices at Via Bistolfi no. 35, Milan, where the research and development laboratories also operate.

The company's governance structure
IDN adopts a "traditional" administration and control system in accordance with Art. 2380-*bis* et seq. of the Italian Civil Code.
The governance structure is based upon the following Bodies:

- Shareholders' Meeting: the Body that expresses, through its resolutions, the will of the shareholder; the shareholders' meetings are the opportunity to establish productive dialogue between the Shareholder and the Directors in the presence of the Board of Statutory Auditors.
- Board of Directors: appointed by the Shareholders' Meeting, this is the Body that oversees the strategic decisions, corporate policies and the definition of the corporate objectives; it is entrusted management of the business in order to achieve the corporate purpose. The Board of Directors is in charge of the functions and related responsibilities in relation to strategic and organisational guidelines, as well as for checking that the necessary controls are in place to guarantee the fairness and legitimacy of the company's actions.
- Chairman of the Board of Directors and managing directors: the persons delegated specific powers by the Board of Directors to administer and manage the business in accordance with the provisions of law and the Articles of Association.
- Board of Statutory Auditors: the body having supervisory functions in relation to compliance with the law and the Articles of Association, as well as management control. The Board of Statutory Auditors, as part of the duties entrusted to it by law, oversees, with the support of the company control structures, the actual functioning of the internal control system and verifies the adequacy of the organisational, administrative and accounting structure approved by the Board of Directors, to which it reports any anomalies or weaknesses.

The bodies tasked with overseeing the company, vested with particular characteristics of independence and autonomy, also include:

- the Independent Auditor, responsible for checking that the accounts are kept properly and that management events have been correctly recorded in the accounting records. In particular, it produces a specific report expressing an opinion on the annual and consolidated financial statements.
- The Supervisory Body (as detailed below, page 20 et seq.) monitors compliance with and actual implementation of this Model, manages and monitors the training and information initiatives for

disseminating awareness and understanding of the Model within the company and among parties operating in its interest, and proposes adaptations and updates to the Model (e.g. following changes to the company's organisation and activities, amendments to the relevant regulatory framework, anomalies or confirmed infringements of the provisions of the Model).

GENERAL PRINCIPLES OF CONTROL

IDN identifies the following main principles to be complied with, as specific tools for planning the formation and implementation of the Company's decisions and for guaranteeing suitable supervision thereof, including in relation to the prevention of crimes:

- assignment of responsibilities: job descriptions and organisational charts with clear reporting flows;
- delegated powers and powers of attorney: assignment of delegated powers and powers of attorney that reflect the management responsibilities with the assignment of consistent powers of representation and aligned and never unlimited spending powers;
- manual and computerised procedures: the presence of adequate Company provisions to supervise sensitive areas in compliance with the principles of segregation of roles, traceability and control;
- segregation of roles: separation within each process between the decision-making party, the executing party and the party responsible for process control;
- reporting and traceability: the demonstration, through precise document tracking, of how a specific Company event or decision-making process unfolds;
- communication and training: the provision of courses on the contents of the Code of Ethics and the Model;
- periodic information flows to the SB: the sending of periodic reports to the Supervisory Body by the Company functions most at risk;
- periodic information flows to the Board of Statutory Auditors;
- periodic information flows to the Board of Directors;
- third-level control: independent checks of the activities/processes carried out by non- operating functions or specialised companies.

Integrated organisational structure documentation

The Company's organisational structure is represented and formalised completely and comprehensively through an organisation chart, organisational communications and intercompany contracts.
This set of documentation clearly identifies all organisational units and their respective duties and responsibilities and the hierarchical and functional reporting flows.

In this regard, in order to realise the synergies existing within the Group in terms of efficient use of skills and streamlining the use of the central structures, IDN provides certain organisational unit activities established internally (such as Legal, ICT, AFC, HR, Procurement) to its subsidiaries.

To guarantee the necessary characteristics of independence, autonomy and authority, the aforementioned Departments operate under specific contracts between related parties signed between IDN and the subsidiaries, regulated at arm's length.

The Company **organisation chart** is attached to this document.

System of Delegations
The Board of Directors has approved the System of Delegations, and constantly monitors its respective adjustment in order to guarantee:

- clear identification and specific delegation of powers and limitations to persons whose actions commit the company and manifest the company will;
- consistency of the delegated powers with the assigned organisational responsibilities;
- adequate periodic reporting mechanisms of the activities conducted under delegated powers.

Integrated internal regulatory system
The Company's overall system of internal rules clearly, congruously and comprehensively regulates all relevant operating methods.
The Policies, issued by the Board of Directors, define the guidelines in relation to governance, organisation and internal control and risk management and in relation to the core business activities.
The procedures and other regulatory instruments adequately regulate the processes and work flows:

- identifying the operating methods and information flows;
- guaranteeing the formal documentation of the activities and the possibility of their *ex post* reconstruction as well as monitoring and line control;
- clearly identifying the process responsibility;
- guaranteeing the segregation of duties and responsibilities;
- guaranteeing accessibility and awareness through adequate information and training activities on the company regulations.

In this respect, the Company has adopted the Group **Code of Ethics** (also attached to this Model) which summarises the fundamental ethical values that inspire the De Nora Group and with which all employees and external collaborators must comply in carrying out the duties entrusted to them, establishing, to monitor the same, an Ethics Committee having specific powers of control regarding the actual application and compliance with the principles indicated therein.

Risk mapping
Art. 6, paragraph 2, letter a) of Italian Legislative Decree 231/2001 indicates, among the requirements of the model, the identification of the processes and activities in the area of which the crimes likely to determine corporate liability may be committed.

Prior to identifying the "at risk" areas within the Company, an analysis - mainly documentary (but not only) - is performed of the corporate and organisational structure of IDN, with the aim of identifying the company areas that form the subject of the intervention. To this end, an inventory is made of the company processes and the procedures that already exist in the potentially "sensitive" areas with reference to the types of crime regulated by the Decree.

Having identified the key persons able to provide operational support in mapping operations, the identification of at-risk processes/activities continued through a series of interviews with persons operating in the area of the relevant company functions, with the aim of analysing the management processes and active control instruments for each sensitive activity.

Any analysis of the risk profiles of the offences of manslaughter and accidental injury committed in breach of the workplace safety regulations has been conducted, taking into account the Risk Assessment

Document drafted pursuant to Art. 17 of Italian Legislative Decree No. 81 of 2008, as well as all the procedures and operating instructions already formalised within the Company.

SUPERVISORY BODY (SB)

Identification of the SB

Art. 6, paragraph 1 of the Decree envisages that the Entity may be exempt from liability if it proves, inter alia, that the duty to oversee the functioning and compliance with the organisation and management model and to deal with its update was entrusted to a Body of the Entity, having autonomous powers of initiative and control.

The IDN SB is a collegiate body composed of three members (one of whom may also be an internal member), appointed by the Board of Directors and chosen from persons with proven professionalism and integrity, and specific skills in relation to audit, administration-management and legal issues. The duration of the mandate is established at the time of appointment.
If the relationship of one of the SB members is revoked or terminated during the mandate, the Board of Directors shall replace him/her without delay.

Any person who has been subject to a final criminal conviction ruling[17] that involves disqualification, temporary or permanent, from public office or from management roles in legal entities, as well as anyone who has been convicted, even if not yet final, of one of the crimes indicated in Italian Legislative Decree no. 231/01 are ineligible for the role of member of the SB (or, if occurring at a later date, constitute just cause for termination of office).

The director with delegated powers and shareholders who, in a senior position, perform functions and activities among those most subject to the supervision and assessment of the SB may not be appointed as members of the SB.

The external members of the SB must not have and/or have had direct economic and commercial relationships with the Company that might jeopardise their autonomy; they may not be connected by a family link or kinship with parties that have (or have had) such relationships with the Company, nor with parties that hold top management functions within it.

At the time of election, the appointed persons will issue a specific declaration of not being subject to any of the indicated causes of ineligibility.

SB prerogatives and resources

For the exercise of its functions, the SB has full organisational and financial autonomy.

To that end, at the start of each financial year, the SB agrees with the Board of Directors the amount of resources required for its activity. The management, use and allocation of such resources are then decided by the SB entirely autonomously and independently.

The SB may collaborate with other persons belonging to the Company if their knowledge and specific expertise is required.

[17] The application of a plea bargain pursuant to Art. 444 of the Italian Code of Criminal Procedure is understood to be equivalent to a conviction ruling.

In cases of particular need, the SB will have the right to obtain advice from external professionals, to whom it may delegate limited areas of investigation.

SB functions and powers

The SB is entrusted on a general level with the duty to oversee:

a) compliance with the requirements of the Model and the documents related to it by the recipients, taking any necessary initiative;
b) the actual effectiveness and capacity of the requirements of the Model, in relation to the company structure, to prevent the commission of the crimes indicated in the Decree;
c) the opportunity to update the provisions and rules of conduct of the Model.

In particular, the SB will achieve the aforementioned purposes through:

- the activation and performance of any control activity considered appropriate;
- scrutiny of the Company's activity, for the purposes of updating the mapping of the at-risk activity areas;
- implementation of any suitable initiative to facilitate the raising of awareness and understanding of the Model by the Company representatives, shareholders, employees and any external collaborators;
- collection, investigation and storage of information received by it;
- coordination with other company functions;
- ascertainment of any possible violation of the requirements of this Model and/or the Decree and the proposal to start any disciplinary proceedings;
- reporting to the Board of Directors of any deficiencies of the Model and consequent proposal of any appropriate modification or improvement;
- collection of reports of conduct or situations in contrast with the provisions of the Model and the implementing procedures of the same, along with any circumstance potentially likely to facilitate or in any case make possible the commission of the crimes or relating to crimes already committed.

INTERNAL INFORMATION FLOWS

Reporting obligations to the SB

Art. 6, paragraph 2, letter d) of the Decree establishes that the Organisation and Management Models must envisage specific reporting obligations to the Body in charge of overseeing the functioning and compliance with the Model, namely the SB.

In addition to any documentation expressly indicated in each Special Section of the Model, all information concerning the following must always be communicated to the SB:

- requests for legal assistance sent by the shareholders, by the members of the corporate bodies and by employees being prosecuted before the court for crimes cited by the Model;
- measures and/or information originating from Judicial Police bodies or from any other authority, revealing the conduct of investigations, also against unknown persons, for the crimes cited by the Model;
- disciplinary proceedings initiated in relation to violations of this Model and any sanctions applied;

- request for, payment and use of public contributions and/or financing of any kind;

The Board of Directors and other corporate bodies are required to provide full details to the SB on issues that fall within its purview.

The Company's shareholders and representatives are required to give the SB prompt notification of any anomaly detected in the conducting of company activities, in relation to at-risk activities, as well as of any subsequent measures adopted.

In particular, the SB has the power to receive useful information for the fulfilment of its duties from each Recipient of the Model, in full autonomy and absolute independence.

Furthermore, the SB has the right to access all company information and documents useful for fulfilling its duties. All Recipients of the Model are required to collaborate in this respect.

All Recipients of the Model must communicate to the SB all information and data relevant for the purposes of preventing the sensitive types of crime pursuant to Italian Legislative Decree 231/01, the adequacy, update and compliance with the Model.

The SB receives the following flows:

- **periodic and continuous information flows (quarterly reports);**
- **specific information flows (envisaged by the individual Special Sections of the Model);**
- **generic information flows.**

The failure of/delayed/unjustified transmission of information flows constitutes a violation of the Model and a disciplinary offence which may be duly sanctioned. In this regard, the SB may suggest to the Board of Directors that disciplinary proceedings be brought against anyone who breaches the reporting obligations identified.

Periodic and continuous information flows

The periodic and continuous information flows to the SB are sent quarterly through reports on a specific form prepared by the Company, based on specific instructions laid down in this regard by the SB, which differ according to the different company functions: these are reports of general and summary nature of what has already been communicated promptly to the SB during the quarter.

The report supplements (and does not replace) the specific and generic information flows that each Recipient is required to make in compliance with the provisions of the Model; the report must be completed and signed by the heads of the company functions involved in the areas most at risk and spontaneously sent to the SB, accompanied by any annexes, within fifteen days of the end of each calendar quarter of reference (i.e. between the 1st and 15th of the months of April, July, October, January).

Specific information flows

The Recipients must communicate to the SB all information and news required by the specific Special Sections of the Model.

Generic information flows
In addition to any documentation expressly indicated in each individual Special Part of the Model, all information that may be relevant for preventing the sensitive types of crime in accordance with Italian Legislative Decree 231/01 and/or for assessing the adequacy of the Model, as well as its update, must always be communicated without delay to the SB.

By way of example but without limitation, the following must be communicated:

- changes to the company's organisational structure;
- renewals or obtaining of new certifications;
- accidents, near misses, incidents, occupational diseases, suspected occupational diseases and/or other anomalies in relation to accident prevention;
- requests for legal assistance sent by the shareholders, by the members of the corporate bodies and by employees being prosecuted before the court for crimes cited by the Model;
- measures and/or information originating from Judicial Police bodies or from any other authority, revealing the conduct of investigations, also against unknown persons, for the crimes cited by the Model;
- disciplinary proceedings initiated in relation to violations of this Model and any sanctions applied;
- request for, payment and use of public contributions and/or financing of any kind;
- local or national news that may be significant in relation to the prevention of criminal acts of a sensitive nature pursuant to Italian Legislative Decree 231/01;
- any other information considered useful for improving the Model.

Information flow communication channels
All information flows must be sent to the SB, either:

- electronically, by sending an email to the SB email address: ODV_IDN@legalmail.it (communicated by the Company by sufficient means of dissemination, such as internal circulars or by affixing notices on the company notice boards);
- on paper, by delivery to the SB on the occasion of meetings held by the same at the Company (if compatible with the timescales/deadlines set for sending the respective information flow),
- by any different methods indicated by the SB itself.

Whistleblowing regulations (Italian Law no. 179 of 30.11.2017)
Italian Law no. 179 of 30.11.2017 laying down "Provisions for the protection of those making reports of crimes or irregularities of which they have become aware as part of a public or private relationship" introduced into the legal system some measures aimed at facilitating the reporting by employees of any crimes committed within the company, particularly through the establishment of procedures aimed at preserving the confidentiality of the whistleblower's identity and the content of the report.

In particular, all Recipients must send to the Supervisory Body, in order to protect the Company, detailed reports of significant illegal conduct in accordance with Italian Legislative Decree 231/01, based upon

precise and consistent factual elements, or reports of any violations of this Model, based upon precise and consistent facts, of which the same have become aware as a result of the functions performed.
This obligation is in addition to (and does not replace) the duty to report to the Ethics Committee, also anonymously, any violation of the Code of Ethics via the page specifically set up on the company portal.

Content of the report
The reports must contain at least the following elements:

- personal details of the individual making the report, indicating the position or role within the Company;
- clear and complete description of the facts being reported;
- circumstances of time and place in which the reported facts occurred (if known);
- personal details or other information identifying the person who perpetrated the reported facts;
- any other useful documents or information to evidence the reported facts.

Reports may be made anonymously as long as they are adequately documented[18].

It is prohibited to submit, with wilful intent or gross negligence, groundless reports.

Any violation of the prohibition, along with any failure to report, constitutes a disciplinary offence and, as such, may be sanctioned in accordance with the disciplinary system of this Model.

Personal grievances may not form the subject of reports[19] and will not be accepted.

Reporting channels
In order to guarantee the confidentiality of the whistleblower's identity, specific reporting channels to the SB are put into place.

All reports must be sent to the SB, either:

- electronically, by sending an email to the SB email address: ODV_IDN@legalmail.it (communicated by the Company by sufficient means of dissemination, such as internal circulars or by affixing notices on the company notice boards); In order to protect the whistleblower's confidentiality, the SB's mailbox is held on a domain external to the company domain;
- on paper, by sending the report in a sealed envelope to the Supervisory Body by ordinary post to the registered office of IDN at Via Bistolfi no. 35, Milan;
- verbally, by means of a personal discussion with the SB during meetings held by the same at the Company, or by requesting an appointment for this purpose.

The whistleblower adopts the communication channel considered most suitable with respect to the nature, urgency and content of the report, favouring, where possible, the electronic method.

Measures to protect the whistleblower
The SB is obliged to maintain the confidentiality of the whistleblower's identity, subject to express authorisation of the person involved.

[18] Confindustria "*Whistleblowing Rules*" - Explanatory Note January 2018.
[19] *Guidelines for preparing Whistleblowing Procedures* - Transparency International Italia (Anti-Corruption Association).

Acts of retaliation or discrimination, direct or indirect, against the whistleblower for reasons connected directly or indirectly to the report are prohibited.[20]

The application of the disciplinary system against any whistleblower who makes groundless reports, with wilful intent or gross negligence, does not constitute an act of retaliation. Any ascertainment of the whistleblower's wilful intent or gross negligence involves the loss of their right to confidentiality, leading to implementation of the disciplinary system.

Any violation of the measures protecting the whistleblower constitutes a violation of the Model and, as such, may be sanctioned in accordance with the disciplinary system of this Model.

SB activities consequent to the report

Reports that are manifestly generic or irrelevant (not containing, for example, a description of specific and concrete facts or referring to illegal facts and/or irregularities not falling within the scope of application of Italian Legislative Decree 231/01) will be archived immediately. The other reports will be assessed by the Supervisory Body, which may request from any Company representative any type of information and/or documentation that may be useful for its investigation and control activity. The request recipient must comply, with the utmost care, completeness and promptness, with any request received by them in that sense from the SB.

A specific report will be drawn up of the investigation activities carried out by the Supervisory Body.

At the end of the investigation activities, if the report is found to be groundless, the Supervisory Body will archive the report.

If the report is, on the other hand, worthy of investigation, the Body will provide a suitable report to the Board of Directors and to the Board of Statutory Auditors.

Any information and/or report received (including those archived) as well as reports of the assessments made by the SB will be stored, by the Body itself, in a specific archive.

Relationships between the SB and the corporate bodies

The SB will inform the Board of Directors, in an annual report, of the activity performed in the period, with particular reference to the verifications performed, indicating any anomalous situations identified during the year, and formulating proposals as necessary for improvement of the company organisation

[20] In this regard, Art. 6, paragraphs 2-ter and 2-quater of Italian Legislative Decree 231/01, establishes the following:
2-ter. *The adoption of discriminatory measures against persons making the reports indicated in paragraph 2-bis may be reported to the National Employment Inspectorate, in order for it to take the measures under its remit, as well as by the whistleblower, also by the trade union organisation indicated by the same.*
2-quater. *Any dismissal by way of retaliation or discrimination against the whistleblower is invalid. Any change of duties in accordance with Article 2103 of the Italian Civil Code is also invalid, as are any other retaliatory or discriminatory measure adopted against the whistleblower. It is the responsibility of the employer, in the case of disputes linked to the application of disciplinary sanctions, or to demotions, dismissals, transfers or subjection of the whistleblower to another organisational measure having direct or indirect negative effects on working conditions, after the submission of the report, to demonstrate that such measures are based upon reasons unrelated to the report itself.*

or of parts of the Model in order to best prevent the risk of committing the crimes envisaged by the Decree.

The SB must in any case promptly report to the Board of Directors any violation of the Model considered to be well-founded, of which it has become aware by way of a report by employees or which the Body itself has ascertained during its supervisory activity.

The Board of Directors and its Chairman have the right to convene the SB at any time which, in turn, has the right to request convocation of the aforementioned body for urgent reasons.

Relationships between the SB and the Board of Statutory Auditors
At least on a half-yearly basis, a meeting must be held between the Board of Statutory Auditors and the SB to exchange information on the performance of their respective roles and the activities within their remit .

This is subject to the possibility of holding additional meetings if this becomes necessary as a result of events and/or reports that require a specific meeting, subject to the duty of mutually reporting anomalies under their common remit.

Relationships between the IDN SB and the DNIT and DNWT SBs
IDN exercises management and coordination over De Nora Italy Srl and De Nora Water Technologies Italy Srl. Each of the latter two companies has appointed its own SB.

At least on a half-yearly basis, a meeting must be held between the aforementioned SBs to exchange information on the performance of their respective roles and the activities under their limited remit.
This is subject to the possibility of holding additional meetings if this becomes necessary as a result of events and/or reports that require a specific meeting, subject to the duty of mutually and promptly reporting anomalies within their shared remit.

Relationships between the SB and other entities
Relationships with the HPPS
At least on a half-yearly basis, a meeting must be held between the SB and the HPPS to carry out monitoring of that envisaged in Special Section - Chapter 5 (Crimes in relation to Workplace Safety) of this Model. The HPPS also sends to the SB on a half-yearly basis a specific report on workplace safety with regard to the status of the prevention measures adopted in the company, any critical areas identified in the period of interest, and the improvement actions taken and/or to be taken.

This is subject to the possibility of holding additional meetings if this becomes necessary as a result of events and/or reports that require a specific meeting, subject to the duty of mutually and promptly reporting anomalies within their shared remit.

Relationships with the Ethics Committee
At least on an annual basis, the SB makes contact with the Group Ethics Committee in order to exchange, within their relative scope of competence, the necessary information regarding performance of the respective assignments. This is subject to the possibility of additional contacts and/or meetings if this becomes necessary as a result of specific events and/or reports.

Relationships with the internal company representative
The Company, having liaised with the SB, may appoint an internal representative, where issued with a prior request, to participate in SB meetings, as well as to coordinate the Recipients, on specific request from the SB, in order to best support the SB in its activities and to promote the fulfilment, within the Company, of the requirements stated and minuted by the SB during its activities, in accordance with Italian Legislative Decree no. 231/01.

DISCIPLINARY SYSTEM

General principles

In light of the provisions of Art. 6, paragraph 2, letter e) of the Decree, a fundamental element for the effectiveness of the Model is the establishment of a sanction system for any violation of the rules of conduct imposed by it.

The establishment of adequate disciplinary measures aimed at preventing and, where necessary, sanctioning any violations of the rules indicated in this Model in fact constitutes an integral and fundamental part of the Model itself and is aimed at ensuring that it is effective. To this end, the Company has established a comprehensive disciplinary system (which is attached to this document, and to which reference is made for any further information).

The application of the disciplinary system and the respective sanctions is independent from the conduct and outcome of any criminal proceedings brought by the Judicial Authority, if the conduct to be censured also constitutes a type of crime that is relevant in accordance with the Decree.

The disciplinary sanctions will be commensurate with the level of liability of the perpetrator of the infringement, any existence of disciplinary precedents for the same, the severity of the conduct, as well as the intentional nature of the same.

The following types of conduct (the list of which is not exhaustive of the types of disciplinary offences) constitute violations, subject to disciplinary sanctions:

- failure to comply with the general rules of conduct and procedures envisaged by the Model, also if implemented through omissions and aided by others;
- preparation, also in conjunction with others, of incomplete or untrue corporate documentation;
- assistance, by way of omissions, in the preparation, by others, of incomplete or untrue documentation;
- violation of the protection measures envisaged by law for those who, in order to protect the integrity of the entity, have made detailed reports of illegal conduct based upon precise and consistent facts, and/or violations of the Organisation and Management Model of the entity, of which they have become aware based upon the functions performed;
- reports of illegal conduct made with wilful intent or gross negligence and which are found to be groundless.
- any other conduct, committed or omitted, that harms or endangers the Company's interest in the effective implementation of the Model.

Having ascertained the violation, the perpetrator will be subjected to a disciplinary sanction proportionate to the severity of the violation committed and to any re-offence.

Any violation of the Model, which may determine the application of a disciplinary sanction, must be notified to the SB, except where the violation has been identified by the same.

The SB has, in any case, the power to launch disciplinary proceedings in relation to conduct constituting violations of the requirements of this Model.

Sanctions against the Directors
If violations of the Model are committed by one or more Directors, the SB will inform the entire Board of Directors, the Sole Auditor and the Shareholders' Meeting; the latter will take the appropriate initiatives envisaged by the Articles of Association and by legislation in force.

If disciplinary sanctions are adopted, the SB must be informed.

Sanctions against the Auditor
If violations of the Model are committed by the Auditor, the SB will inform the entire Board of Directors, which will take the appropriate initiatives envisaged by the articles of association and by the legislation in force.
If disciplinary sanctions are adopted, the SB must be informed.

Sanctions against employees
If violations of this Model are committed by one or more directors, the SB will immediately inform the Company's Board of Directors and Board of Statutory Auditors. Conduct in violation of the rules contained in this Model will constitute a disciplinary offence and will be sanctioned as envisaged in the disciplinary system approved by the Company, and, more generally, in the National Collective Labour Agreement for the industry.
If disciplinary sanctions are adopted, the SB must be informed.

Measures against external collaborators and Partners
Any conduct adopted by external collaborators, or by industrial and/or commercial partners, in conflict with the code of conduct indicated in this Model and in any case likely to involve the risk of committing one of the crimes indicated in the Decree, may determine, as envisaged by the specific contractual clauses inserted in the engagement letters or agreements, the termination of the contractual relationship.

DISSEMINATION AND AWARENESS OF THE MODEL IN THE COMPANY

Staff training
In order to ensure the most effective application of this Model, the SB shall spread awareness of the Model and its provisions within the Company, by distributing the text on paper or electronically (*e -mail or My Governance Company platform*), as well as through any other suitable information and awareness-raising initiatives (including publication on the www.denora.com website).

Similarly, the Company will disseminate all additions and modifications that are made to the Model over time.

In particular, all company functions must be trained on:

- Italian Legislative Decree 231/01 and its consequences in relation to corporate liability;

- the types of crime envisaged and punished by the combined provisions of Italian Legislative Decree 231/01 and the types of crime cited therein;
- the analysis of the risk areas of the aforementioned crimes;
- the analysis of the prevention protocols envisaged within the Special Sections of this Model;
- the essential principles of the rules on whistleblowing (Italian Law no. 179 of 30.11.2017) and notably:
- relevant regulatory context;
- material operation and methods of accessing the information channels established to ensure that the reporting system functions correctly;
- the sanction system established for those who violate the whistleblower protection measures, as well as those who, with wilful intent or gross negligence make reports that are considered to be groundless.
- communication channels of periodic and continuous, specific and generic information flows envisaged by this Model;
- sanction mechanisms envisaged in the event of violation of the requirements contained in this Model.

To that end, the information must be complete, prompt, accurate, accessible and continuous, so as to allow all shareholders, representatives and employees of the Company to gain full awareness of the company directives and be placed in a position to respect them.

All course Recipients[21] must undergo - via the De Nora Academy portal - a personal learning assessment test, consisting of multiple choice questions on the course subjects. In the event of amendments to the Model and/or new legislative provisions and/or changes to the company's organisation, specific new training sessions and meetings may also be introduced.

Any unjustified failure to organise and/or participate in the training course will constitute an infringement of this Model, triggering the disciplinary system.

The SB will verify, also by sampling methods, that all recipients within the Company are effectively aware of the Model.

New employees will receive a copy of this Model, upon recruitment and from the Head of Human Resources, via the *My Governance* company portal. The system certifies the receipt, as well as the commitment by the new recruit to comply with the contents of the same.

A paper copy of this Model will remain available to employees at the HR Department at Via Bistolfi no. 35, Milan.

Information to external collaborators and partners

The Company promotes awareness and compliance with the Model also among the commercial and/or industrial *partners* with which it holds significant financial relationships, as well as among external

[21] Senior bodies and control bodies are excluded, as the training reserved for them is at a different level to the other recipients. By way of example, the course for senior bodies and control bodies may take place during a meeting with the SB.

collaborators, who are not employees of the same. These will be informed of the content of the Model, also by extract, from the very start of the professional or commercial relationship.

PERIODIC CHECKS

The SB must carry out periodic checks (no less than four times a year and in any case whenever necessary) aimed, in particular, at:

- overseeing the functioning of and compliance with the Model by all persons who operate within the Company and on behalf of the same;
- obtaining any useful information for making proposals in relation to the updating of the Model;
- ascertaining the effective suitability of the Model to prevent the commission of crimes;
- checking the constant adequacy of the information channels established for reporting significant illegal conduct in accordance with Italian Legislative Decree 231/01 and/or violations of this Model as envisaged by the regulations on whistleblowing (Italian Law no. 179 of 30.11.2017);
- guaranteeing compliance with the prohibition on acts of retaliation or discrimination, direct or indirect, against whistleblowers for reasons connected, directly or indirectly, to the report;
- verifying the correct use of information channels by those reporting the committing of criminal offences and/or violations of this Model.

The SB analyses all reports received, events considered at risk and information and training initiatives implemented to disseminate, at all company levels, awareness of the provisions of the Decree and this Model.

The outcomes of the checks performed and any critical areas found must be reported to the Board of Directors, at its next meeting, indicating, if appropriate, any adjustments to be made.

SPECIAL SECTION

CHAPTER 3

CORPORATE CRIMES

In reforming the area of "corporate crimes" (art. 2621 et seq. of the Italian Civil Code), Italian Legislative Decree No. 61/2002 introduced a new article to the text of the Decree (Art. 25-ter), which extended the administrative liability of legal entities to the commission of "the corporate offences provided for in the Civil Code, if committed in the interests of the Company, by directors, general managers or liquidators or persons under their supervision, where the crime would not have been committed had it been monitored in compliance with the obligations relating to their respective remits".

The corporate activities of IDN S.p.A. are subject to supervision by the Board of Statutory Auditors and the Independent Auditor.

The corporate criminal offences likely to affect the activity of IDN, a company not listed on regulated markets and not subject by law to the control of public supervisory authorities, can be split into three categories:

- crimes related to economic, financial and capital information relating to the financial statements, reports or other corporate communications envisaged by law and, in particular:
  - false corporate communications (Art. 2621 and Art. 2621-bis of the Italian Civil Code);
- crimes relating to the management of corporate governance and, in particular:
  - impeded control (Art. 2625 of the Italian Civil Code);
  - undue return of contributions (Art. 2626 of the Italian Civil Code);
  - illegal allocation of profits and reserves (Art. 2627 of the Italian Civil Code);
  - illegal transactions on company stocks or shares or those of the parent company (Art. 2628 of the Italian Civil Code);
  - transactions prejudicial to creditors (Art. 2629 of the Italian Civil Code);
  - fictitious formation of capital (Art. 2632 of the Italian Civil Code);
  - undue allocation of company assets by liquidators (Art. 2633 of the Italian Civil Code);
  - unlawful influence on the shareholders' meeting (Art. 2636 of the Italian Civil Code).
- crime of corruption and incitement to corruption among private entities (Art. 2635 and Art. 2635-bis of the Italian Civil Code)

A brief description of the aforementioned crimes is provided below:

False corporate communications (Art. 2621 and Art. 2621-bis of the Italian Civil Code) – Art. 2621 of the Italian Civil Code is intended to protect the trust placed by shareholders and creditors in the truthfulness of the financial statements and communications of the enterprise, organised in corporate form, irrespective of whether or not they incur damage and even if no damage is incurred (Art. 2621-bis of the Italian Civil Code envisages mitigation for acts of minor significance). The crime punishes the illustration of material facts that are untrue or the omission of material facts the communication of which is required by law with reference to the economic, capital and financial situation of the company.

Impeded control (Art. 2625 of the Italian Civil Code) – This crime occurs when, by concealing documents or through other deception, the conduct of the control activities legally attributed to the corporate bodies is impeded or hindered.

Undue return of contributions (Art. 2626 of the Italian Civil Code) – This crime materialises when the directors, with the exception of cases of legitimate share capital reduction, return, also by simulation, contributions to the shareholders or release them from the obligation to make them.

Illegal allocation of profits and reserves (Art. 2627 of the Italian Civil Code) – This crime materialises when, except where the circumstance constitutes a more serious crime, the directors allocate profits or advances on profits not actually attained or intended by law for the reserve, or they distribute reserves, also not formed from profits, which cannot, by law, be distributed. The return of the profits or the reconstitution of reserves before the deadline set for the approval of the financial statements extinguishes the crime.

Illegal transactions on company stocks or shares or those of the parent company (Art. 2628 of the Italian Civil Code) – This crime materialises when the directors, outside the cases permitted by law, purchase or subscribe company stocks or shares, causing damage to the integrity of the share capital or the reserves that cannot be distributed by law; or, outside the cases permitted by law, they purchase or subscribe stocks or shares issued by the parent company, causing damage to the share capital or reserves not distributable by law. If the share capital or reserves are reconstituted before the deadline set for the approval of the financial statements for the financial year in relation to which the conduct was implemented, the crime is extinguished.

Transactions prejudicial to creditors (Art. 2629 of the Italian Civil Code) – This crime materialises if the directors, in violation of the legal provisions protecting creditors, make share capital reductions, or perform mergers with other companies or demergers, causing damage to creditors.

Fictitious formation of capital (Art. 2632 of the Italian Civil Code) – This crime materialises when the directors and shareholders of the Company, also in part, form or increase fictitiously the share capital by attributions of stocks or shares in an amount higher than the sum of the share capital, reciprocal subscription of stocks or shares, significant over-valuation of the contributions of assets in kind or credits or the equity by the Company in the case of transformation.

Unlawful influence on the shareholders' meeting (Art. 2636 of the Italian Civil Code) – This crime materialises when a person, with simulated or fraudulent acts, such as by promising a participant in the shareholders' meeting an economic advantage, determines the majority in the shareholders' meeting, with the aim of procuring for themselves or for others an unjust profit. The crime materialises with the irregular formation of a majority.

Corruption and incitement to corruption among private entities (Art. 2635 and Art. 2635-bis of the Italian Civil Code) – The crime of corruption among private entities punishes the directors, general managers, managers in charge of preparing the corporate accounting documents, auditors, liquidators and anyone who, within the organisation, exercises management functions other than those of the entities mentioned above who - also through a third party - solicits or receives, for themselves or for others, money or other illicit gains or accepts the promise of the same. The possibility of punishment is also extended to those subject to the management or supervision of the persons indicated above. Those who, also through a third party, offer or promise or give money or other gains that are not due are also

punished. In all these cases, the solicitation, offer and/or promise must be made for the purpose of having the interlocutor perform (or omit) an act contrary to official obligations and/or duties of loyalty. For the purposes of the commission of the crime, therefore, the mere promise (or acceptance of a mere promise) of money or illicit gains is sufficient. If the offer or promise is not accepted, the crime of corruption does not materialise, but there is, however, the crime of "incitement to corruption", punished less severely but still included in the category of crimes regulated by Italian Legislative Decree 231/01.

RISK AREAS

In light of the crimes and conduct cited above, the Company's areas of activity considered most at risk of commission of illegal activities can be identified as follows:

A) activity of preparation of communications to the shareholders (or to the public) and in particular:

- management of general accounting;
- management of supplier, customer and employee accounting;
- drafting and preparation of the financial statements, reports and other corporate communications required by law and sent to the shareholders and to the public;
- management of the IT system containing all company accounting data;
- activity of collection, assessment and aggregation of accounting data necessary for preparing the financial statements;

B) relationships with the control body and, in particular:

- communication of necessary periodic information;

C) relationships with the Independent Auditor and, in particular:

- communication of necessary periodic information;

D) management of ordinary and extraordinary transactions;

- management of intercompany relationships;
- management of acts of the Board of Directors;
- management of relationships with shareholders;

E) management of tax obligations;

F) negotiation, stipulation and management of active contracts with private legal entities, even without legal status;

- purchase of goods and services;
- selection, approval and assessment of suppliers;
- management of gifts, hospitality and entertaining expenses;
- management of relationships with financial and credit institutions;
- management of relationships with consulting companies;
- management of relationships with insurance companies;
- management of relationships with private certifying bodies.

The list is obviously subject to changes and additions; if this becomes necessary, additional risk areas will be identified, with consequent preparation of specific rules of conduct and respective procedures.

In such cases, the SB is responsible for proposing to the Board of Directors any appropriate intervention on the text of the previous Special Section. The Board of Directors itself may also take similar initiatives autonomously.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at the directors, the Sole Auditor, the Company shareholders and employees, as well as any external collaborators who take part in one of the processes relating to the at-risk activities highlighted above.

GENERAL CODE OF CONDUCT

The recipients are expressly obliged:

- to behave in a correct, scrupulously transparent and collaborative manner, based upon full compliance with the rules of law in all activities related to and aimed at preparing the financial statements and other corporate communications, with the aim of providing to the shareholders and to third parties true, complete and correct information on the economic, financial and capital situation of the Company;
- to pay the utmost attention and exercise caution, through compliance with the rules of law and internal procedures, to protecting the integrity and effectiveness of the capital and company equity, in full compliance with the guarantees of creditors and third parties in general;
- to take care of and protect the due functioning of the company and the corporate bodies, guaranteeing and facilitating any form of control of company management and guaranteeing the free formation of the will of the shareholders' meeting.

SPECIAL CODES OF CONDUCT RELATING TO THE INDIVIDUAL RISK AREAS

Communications to the shareholders and to third parties

Financial statements and other corporate communications

The activity of preparing the annual financial statements and the management report must take place on the basis of the requirements contained in the document entitled "*De Nora Group – Accounting Standards Manual*". The Company has also adopted a procedure ("*De Nora Group - financial and legal due diligence reports*") aimed at ensuring the preparation of monthly reports, by all Companies belonging to the De Nora Group, on the potential risks of financial or legal exposure. Those reports are sent directly to the corporate, financial and legal departments of Industrie De Nora S.p.A.

The activities linked to corporate information must be based upon the following principles:

- the planning of precise deadlines for all formalities required to prepare the financial statements, guaranteeing the prompt transmission to all members of the Board of Directors and the Sole Auditor of the draft financial statements, appropriately in advance of the approval date;
- in particular, around the same time as the closure of the accounts each year, the procedures and time frames laid down in the operating instruction entitled "SAP: *Period end closing procedure* " must be strictly complied with;
- the IT system used for sending data and information must always ensure the traceability of the individual steps and the identification of the workstations that enter the data into the system;

- the planning of one or more meetings involving the Control Body and the SB, before the meeting of the Board of Directors to approve the financial statements, concerning the assessment of any critical areas emerging in the auditing activity.

It is expressly prohibited for all recipients:

- to represent in the financial statements, reports and statements and, in general, in any corporate communication false, incomplete or untrue information on the economic, capital and financial situation of the Company;
- to omit data and information required by law on the economic, capital and financial situation of the Company.

Management of relationships with the Board of Statutory Auditors

In relation to the conduct of corporate management control activity, the following must be established:

- the timescales and deadlines for prompt transmission to the control body of all data and all information required for the same to best fulfil its control duties;
- the possibility of periodic meetings and discussions between the control body and the SB on matters relating to compliance with the rules and company procedures on corporate governance by the Directors, managers and employees.

It is expressly prohibited to adopt conduct that in any way impedes, by concealing documents or using other fraudulent means, or that in any case hinder the conduct of control activity by the sole auditor.

Management of relationships with the Independent Auditor

With regard, however, to relationships with the Independent Auditor:

- the recipients of the Model must guarantee prompt and complete satisfaction of requests for specific documentation made by the Independent Auditor during its audit and control activities and the assessment of the administrative/accounts processes;
- the data and documents must be made available promptly and in clear and exhaustive language that enables the provision of accurate, complete and truthful information;
- consultancy tasks, concerning non-audit activities, cannot be assigned to the Independent Auditor or to companies or professional entities that are part of its network. Any exceptions must be promptly submitted to the Board of Statutory Auditors for an opinion.

It is expressly prohibited to adopt conduct that in any way impedes, by concealing documents or using other fraudulent means, or that in any case hinders the control and audit activities of the Board of Statutory Auditors and the Independent Auditor.

Protection of share capital

All transactions that, directly or indirectly, may affect the share capital, such as the distribution of profits and reserves, the purchase or sale of investments or business branches, mergers, demergers or spin-offs, must occur with the following measures:

- the single body in charge of making decisions on significant transactions is the Board of Directors, without prejudice to the responsibilities of the shareholders' meeting;
- if requested by the SB, the entire documentation relating to any transaction must be provided to it immediately;

- it must be possible for a meeting and a discussion to be held between the Sole Auditor and the SB in relation to the transactions in question.

It is expressly prohibited:

- to return contributions to the shareholders, also by simulation, or to release them from the obligation of making such contributions, outside the scope of cases of legitimate reduction of the share capital;
- to distribute profits or advances on profits not actually achieved or to be allocated by law to a reserve;
- to purchase or subscribe shares of the Company or subsidiaries outside the scope of cases envisaged by law, harming the integrity of the share capital;
- to make reductions of the share capital, perform mergers or demergers, in violation of the provisions of law protecting creditors;
- to proceed with the formation or fictitious increase of the share capital, allocating shares for a value less than their nominal value at the time of the share capital increase.

Management of intercompany transactions

The management of intercompany transactions is regulated by specific procedures on intercompany operations that are aimed at illustrating the methodology adopted by the Company in relation to the management of intercompany transactions, identifying - in particular - the different categories of intercompany counterparties, the criteria and methods by which the transactions are to be performed, the types of transactions identified and the respective decision-making processes and corporate governance mechanisms adopted by the Company.

The intercompany transactions respect criteria of transparency and substantial and procedural fairness and they are implemented consistently with principles of sound and prudent management (substantial fairness means the fairness of the transaction from a financial perspective; procedural fairness means the compliance with procedures aimed at guaranteeing the substantial fairness of the transaction).

Intercompany transactions are implemented at market conditions or if the fee is correlated adequately to the service, based upon current price and/or rate parameters, for transactions similar to those usually applied to unrelated parties for transactions of corresponding nature, amount and risk, or based upon regulated tariffs or imposed prices, or those applied to entities with which the Company is obliged by law to contract at a certain fee. If the nature, value or other characteristics of the transactions so require, assistance may be obtained from independent experts, in order to correctly assess their contractual terms.

All intercompany transactions are traceable and adequately certified by way of suitable documentation, which is stored at a specific internal organisational unit in charge of managing corporate fulfilments in relation to intercompany operations, as well as the collection of information useful for determining the perimeter of entities falling within the category of intercompany counterparties and the update of the respective database.

Corruption among private entities

As part of the management of procurement processes of goods and services, the Parent Company has adopted a system of procedures, binding for all Group companies, aimed at regulating aspects relating to the purchase of goods and services as well as the selection and approval of suppliers and, more precisely:

- *Vendor Master Data Management*;
- *Procurement of Common Items*;

- *Organisational Document System*;
- *Material Master Data Rules*;
- *Titanium Scraps Management*;
- *Vendor Management*;
- *Planning and Procurement of Strategic Items*;
- *Vendor Evaluation*;
- *Vendor Qualifications*;
- *Business Card Management*;
- *Suppliers' Code of Ethics*;
- *Operating Instructions Manual (MOI) - Supplier Qualification and Assessment.*

In any case, it is expressly prohibited to:

- make cash donations to private entities;
- promise or distribute, solicit or receive gifts and presents beyond what is envisaged in normal company practice (i.e. any form of gift offered or received, exceeding normal commercial practices or courtesy, or in any case aimed at acquiring favourable treatment in the conduct of any business activity). In particular, any form of gift to private entities and their relatives that may influence their independence of judgement or lead them to give any advantage to the Company, is prohibited. Gifts that are permitted are always characterised by their negligible value or those aimed at promoting artistic initiatives. Gifts offered - except those of modest value - must be adequately documented in order to facilitate the necessary checks;
- promise or agree other benefits of any nature (promises of recruitment, use of company assets, etc.) in favour of private entities that may lead to the same consequences envisaged in the previous point;
- receive benefits of any nature, exceeding normal commercial practices or courtesy, or in any case aimed at acquiring undue favourable treatment in the conduct of any business activity;
- incur entertaining expenses not based upon criteria of reasonableness or in the absence of actual business purposes;
- make facilitation payments, i.e. unofficial payments of low value with the aim of expediting, facilitating or guaranteeing the performance of a routine activity or in any case forming part of the duties of the private entities with which the Company holds relationships;
- provide services in favour of commercial partners and/or consultants that are not adequately justified in the context of the associative relationship established with the same;
- make payments in favour of external collaborators that are not adequately justified in relation to the type of assignment to be carried out and existing practices.

For the purposes of the implementation of the conduct outlined above:

- the company participates in the cash pooling arrangement implemented by the Parent Company;
- the agreements with Partners and/or other third parties are defined in writing, highlighting all terms of that agreement - with particular regard to the agreed financial terms - and are verified and approved based upon existing procedures and in compliance with the powers granted;
- those who carry out a role of control and supervision of fulfilments related to performance of the aforementioned activities (payment of invoices, allocation of funding obtained from the State or from EU bodies, etc.) must pay particular attention to the implementation of those fulfilments

and report immediately to the SB any situations of irregularity; relationships with subsidiary companies, direct or indirect, must be managed in compliance with principles of management autonomy, fairness, transparency and effectiveness;

- any situations of uncertainty in relation to the conduct to be adopted, in the interpretation of existing legislation and internal procedures must be submitted to the attention of the hierarchical superior and/or the SB.

DUTIES OF THE SB

With regard to prevention and supervision, in relation to the risk of committing corporate crimes, the duties of the SB will be the following:

- in general, the SB will monitor the effectiveness and adequacy of this Special Section, proposing to the Board of Directors the necessary modifications and all adjustments considered appropriate;
- with regard to corporate communications and, in particular, the financial statements, the SB duties are focused on:
  - monitoring the effectiveness and implementation of the internal procedures to prevent crimes of false corporate communications;
  - examination of any report and proposal originating from the corporate bodies, managers or employees and performance of all necessary assessments;
  - constant supervision of the effectiveness of the control implemented by the Sole Auditor;
- with regard to the other at-risk activities:
  - examination of any report and proposal originating from the corporate bodies, managers or employees and performance of all assessments considered necessary.

It is also the duty of the SB:

- to monitor that the heads of the areas at risk of crime are aware of the duties and tasks connected to the control of the area for the purposes of preventing the commission of the crimes in question;
- to verify periodically - with the support of the other competent functions - the system of delegations in force, recommending changes if the power of management and/or qualification does not correspond to powers of representation granted to the internal manager or to the deputy managers;
- to indicate to the Board of Directors any additions to the financial and accounting management system adopted by the Company in order to highlight suitable measures to identify the existence of any atypical financial flows subject to margins of discretion;
- to verify periodically, with the support of the other competent functions, the validity of appropriate standard clauses aimed at ensuring:
  - the observance by external collaborators and partners of the Model and the Code of Ethics;
  - the implementation of sanction mechanisms (such as withdrawal from the contract in relation to Partners or external Collaborators) if violations of the requirements are ascertained.

The Supervisory Body, in carrying out the aforementioned activities, has the right to access all company documentation available in this regard with no obligation to provide prior notice.

CHAPTER 4

CRIMES AGAINST PUBLIC ADMINISTRATION

Articles 24 and 25 of the Decree identify different types of crime that may be implemented as part of relationships with Public Administration.

According to provisions of the Italian Criminal Code:

- in accordance with Art. 357, paragraph 1 of the Italian Criminal Code, *public officials* are considered to be those who exercise a public legislative, judicial or administrative function;
- in accordance with Art. 358 of the Italian Criminal Code, "*civil servants*" are those who, in any capacity, are permanent staff of the Civil Service. The activity of a civil servant is regulated in the same manner as a public official, but characterised by the absence of powers typical of the latter, and excluding the conduct of simple ordinary duties and the performance of merely material work.

Below is a brief description of the crimes that could be committed as part of the activity performed by IDN:

Misuse of money to the detriment of the State (Art. 316 *bis* of the Italian Criminal Code) – This crime materialises when a person, extraneous to Public Administration, has obtained the payment, from the State or another Public Entity or the European Communities, of contributions, grants or funding intended for the implementation of works or the conduct of activities in the public interest, but has not used them for those purposes**.**

Undue receipt of payments to the detriment to the State (Art. 316-*ter* of the Italian Criminal Code) – This crime materialises when a person has obtained contributions, funds, assisted loans or other payments of a similar nature, from the State or other Public Bodies or from the European Communities, by using or submitting false declarations or documents or those certifying false facts, or by omitting due information.

Extortion (Art. 317 of the Italian Criminal Code) – This type of crime materialises when the public official, abusing his/her capacity or powers, forces a person to give or promise unduly, to him/her or to a third party, money or other gains.

Corruption in carrying out duties (Art. 318 of the Italian Criminal Code) – This type of crime materialises when a private entity promises or gives unduly to a public official, for itself or for a third party, money or other gains (e.g. a gift in kind) for the exercise of his/her functions or powers (e.g. to give precedence to specific cases over others or to "facilitate/expedite" the case itself). The criminal rule punishes both the corrupted person and the corrupter.

Corruption for an act contrary to official duties (Art. 319 of the Italian Criminal Code) – This type of crime materialises when a private entity gives or promises to a public official, for him/herself or for a third party, money or other gains (e.g. donations in kind) to omit or delay, or to have omitted or delayed, an act of his/her role, or to complete or have completed an act contrary to official duties (for example,

during a tax audit by the Tax Authority, paying or promising sums of money or other assets in kind, to officials of the Tax Police, so that they omit some tax audits). Once again in this case, the criminal rule punishes both the corrupted person and the corruptor.

Corruption in judicial deeds (Art. 319-*ter* of the Italian Criminal Code) – This rule punishes anyone who implements acts of corruption such as those described in the previous rules with the aim of facilitating or damaging a party in civil, criminal or administrative proceedings (usually a magistrate) involving the Company itself or a third party.

Undue incitement to give or promise gains (Art. 319-*quater* of the Italian Criminal Code) – This type of crime occurs when, except where the act constitutes a more serious crime, a public official or a civil servant, in abuse of his/her capacity or powers, induces the employee or representative of the Company to give or promise unduly, to him/her or to a third party, money or other gains. Once again in this case the criminal rule punishes both parties involved.

Corruption of a civil servant (Art. 320 of the Italian Criminal Code) – This type of crime materialises when the corruption in carrying out a duty or through an act contrary to official duties concerns a civil servant.

Incitement to corruption (Art. 322 of the Italian Criminal Code) - This type of crime materialises when a private entity offers or promises money or other illicit gains to a public official or to a civil servant for the exercise of his/her functions or powers, but the offer or promise is not accepted. The crime also occurs also if the promise or offer is made to incite a public official or civil servant to omit or delay an official act, or to perform an act contrary to his/her duties, if the offer is not accepted,

Embezzlement, extortion, undue incitement to give or promise gains, corruption and incitement to corruption of members of the International Criminal Court or the bodies of the European Communities and officials of the European Communities and of foreign countries (Art. 322-*bis* of the Italian Criminal Code) – This type of crime materialises when an employee or representative of the Entity commits crimes of corruption and incitement to corruption towards members of the European institutions (International Criminal Court, European Commission, European Parliament, Court of Justice, Court of Auditors).

Influence peddling (Art. 346-bis of the Italian Criminal Code) – This type of crime materialises when a person makes others give or promise unduly money or other gains, to themselves or to others, exploiting or taking advantage of existing or alleged relationships with a public official or a civil servant or members of the International Criminal Court or the bodies of the European Communities or officials of the European Communities and of foreign countries, as the price for their intermediation towards any one of the entities indicated above or to remunerate any one of them in relation to the exercise of their functions or powers.

Fraud to the detriment of the State or another public entity or the European Union (Art. 640 of the Italian Criminal Code) – This type of crime applies when any person, through artifice or deception (e.g. by producing false documents), misleads the State or a public body, obtaining a profit from the same and causing, at the same time, damage to the State or to the public body.

Aggravated fraud to obtain public funds (Art. 640-*bis* of the Italian Criminal Code) – This type of crime applies when a Company representative, through artifice or deception (e.g. by producing false

documents), misleads the State or a public body or European Institutions, obtaining contributions, funding, subsidised loans or other payments of that nature.

Cyber fraud (Art. 640-*ter* of the Italian Criminal Code) – This type of crime occurs when, by altering in any way, without authorisation, the functioning of an IT system, an unjust profit is obtained in detriment to others.

Fraud in public supplies (Art. 356 of the Italian Criminal Code) – This type of crime occurs in the case of fraudulent execution of a supply contract with the State, public body or enterprise performing a public service, i.e. in the delivery of items or works that do not comply, in whole or in part, with that contractually envisaged.

RECIPIENTS OF THE SPECIAL SECTION

This Special Section is aimed at members of the company bodies, employees operating in at-risk activities, i.e. in relationships with Public Administration, with particular reference to persons involved in research and development activities who occasionally benefit from contributions, subsidies and/or financing from public, state or EU institutions).

It is worth noting that such wording may also include private entities subject to public control which exercise administrative functions, activities related to the production of goods and services in favour of public administrations and/or management of public services[22].

The codes of conduct envisaged therein extend to and must be complied with also by any external collaborators, who, as envisaged in the General Section of the Model, must also be made aware of its content.

RISK AREAS

The crimes considered have as a prerequisite the establishment of relationships with Public Administration (considered in the broad sense and including also subsidiary companies of public administrations in foreign countries).

IDN does not have significant commercial relationships with public entities, either in Italy or abroad; conversely, there may be interactions with public institutions as part of procedures for the granting of loans, subsidies and/or contributions for research and development.

The following must, therefore, be considered at-risk areas:

- management of relationships with public institutions and bodies aimed at the concession of funding, grants and/or contributions for research and development;
- management of relationships with public institutions and entities in relation to requests for administrative measures, licences and authorisations, other communications to public entities;
- management of judicial and extrajudicial litigation;

[22] Cf. ANAC, *Guidelines for the implementation of the rules on preventing corruption, and transparency of companies and private entities controlled and invested by the PA and public financial bodies*, Decision no. 8/2015, in www.anticorruzione.it, 22.

- management of accounting and taxes (tax returns and any controls on the correct keeping of records and on tax amounts);
- administration, finance, accounting, tax (particular attention must be paid to sectors that involve the outgoing payment of funds, such as order management and invoices payable);
- management of consultancy and professional service contracts;

Any additions to the indicated as at-risk areas may always be made by the Board of Directors, also on the opinion and at the proposal of the SB.

CONTROL MEASURES

All sensitive activities must be carried out in compliance with the laws in force, the Code of Ethics, the principles of Corporate Governance of the Company, in addition to the rules contained in this Model.

To that end, IDN has established organisational tools responding to the internal control principles, such as formalisation and clarity, communication and separation of roles, in particular, as regards the allocation of responsibilities, representation and definition of the hierarchical lines of the operating activities.

One of the organisational and control instruments, operating within the Company, is the system of delegations and powers of attorney, which defines the activities and responsibilities of the organisational units, in order to achieve a clearly structured and efficient management of the company activities.

The basic principles of the system of delegations, identifiable in the need to avoid the excessive concentration of powers in a single entity, as well as to separate the responsibilities in duties and in functions, meet the purpose of preventing legal risks, including, *in primis,* the risk of incurring corporate liability resulting from a crime regulated by Italian Legislative Decree 231/01.

"Delegation of power" means the conferment of a power of management, namely the attribution of functions and duties as recorded in the flow chart of company processes, which is constantly updated.

CODE OF CONDUCT

In undertaking and managing relationships with Public Administration (during the management of relationships with the judicial, administrative and financial authorities in requests for and management of authorisations, requests for public funding, licences and administrative concessions, in personnel management, as well as, more generally, in any relationship, direct or indirect, with Public Administration), all those who operate on behalf of the Company must comply with the following principles:

- compliance with the principles of fairness and transparency and guarantee of the integrity and reputation of the parties;
- compliance with laws and regulations in force, ethical principles and existing procedures;
- traceability and documentation of relationships held with public officers;
- personal contacts with public officers must occur exclusively by authorised persons in line with the assigned organisational responsibilities;
- communications sent to Public Administration must be signed in compliance with the powers granted;

- compliance with company responsibilities and the system of delegations in place, also with reference to the expenditure limits relating to the functions and methods of managing financial resources;
- correct use of IT procedures;
- the relationships in question must be managed exclusively by the competent company functions.

In performing the aforementioned activities, it is expressly prohibited for all members of the corporate bodies and employees, directly, and for all external collaborators, by way of specific contractual clauses, to:

- promise or offer, also through a third party, gifts, assets or other gains to public officials or civil servants, in relation to the completion of official acts;
- submit untrue declarations or documentation to national or European public bodies in order to obtain public funding, contributions or subsidised loans;
- make cash payments to public officers;
- allocate sums received from national or European public bodies by way of funds, contributions or loans for purposes other than those for which they were intended;
- agree or even simply promise other benefits of any nature in favour of representatives of Public Administration;
- provide services in favour of Public Administration that are not adequately justified in specific relationships of a contractual nature;
- pay fees in favour of external collaborators that are not adequately justified in relation to the type of assignment that they must perform and that involve a relationship with Public Administration;
- distribute any gift to Italian and foreign public officers or their relatives, which may influence their independence of judgement or lead them to provide any advantage to the company.

Those who are involved in the aforementioned risk areas are required to oversee the fulfilments related to those activities and to report immediately any irregularities or anomalies.
Furthermore, any person responsible for a risk operation must communicate immediately to the SB any "suspicious" situation, meaning any fact or circumstance that has come to his/her attention which presents profiles of irregularity.

In general, except for payments of low value, no payment in cash or in kind is permitted.

Any agreements with companies or external collaborators, such as contracts and letters of appointment to external professionals, must always be in writing (including by e -mail), with a precise indication of the subject; in the agreement, the Company or external collaborator (or legal representative, for a legal entity) or the professional shall declare familiarity with the content of the Model, undertaking to comply with it.

Anyone involved in activities that benefit from public grants, financing and/or subsidies are required to monitor obligations connected with these activities (in particular, with reference to the allocation of sums received from the state or EU bodies) and immediately report any irregularities or anomalies.

All documentation relating to the participation in public tender procedures and requests for concessions, loans and/or public funding, along with all documentation certifying the use of the funds received, must be stored in a specific archive by the head of the relevant structure.

DUTIES OF THE SB

The Supervisory Body has the power to perform specific checks, also as a result of reports received; the Body also has the right to access all company documentation available in the matter, with no obligation to provide prior notice.

The Company has also established, at the request of the Supervisory Body, information flows functional to the acquisition of useful information for monitoring sensitive activities relating to relationships with Public Administration.

In particular, the Supervisory Body must be informed through a written note of any critical area or conflict of interest that has arisen or is arising as part of the relationship with the PA.

It is the duty of the SB:

- to monitor that the heads of the areas at risk of crime are aware of the duties and tasks connected to the control of the area for the purposes of preventing the commission of the crimes in question;
- to verify respect, implementation and adjustment of the Model consistently with the need to prevent the commission of the crimes in question;
- to oversee the effective application of the Model and to identify deviation in conduct that may emerge from the analysis of information flows and reports received;
- to analyse any report that is received in relation to possible violations of this Special Section or relating to the commission of illegal acts or even just "suspicious" acts, preparing a specific report to be sent to the Board of Directors and proposing, if necessary, the adoption of appropriate disciplinary measures;
- to verify periodically - with the support of the other competent functions - the system of delegations in force, recommending changes if the power of management and/or qualification does not correspond to powers of representation granted to the internal manager or to the deputy managers;
- to verify periodically, with the support of the other competent functions, the validity of appropriate standard clauses aimed at ensuring:
    - the observance by external collaborators and partners of the Model and the Code of Ethics;
    - the possibility of performing effective control actions in relation to the Recipients of the Model in order to verify compliance with the requirements contained therein;
    - the implementation of sanction mechanisms (such as withdrawal from the contract in relation to Partners or external Collaborators) if violations of the requirements are ascertained.

The Supervisory Body, in carrying out the activities indicated above, may make use of all competent resources in this regard.

CHAPTER 5

CRIMES IN RELATION TO WORKPLACE SAFETY

Art. 25-septies of Italian Legislative Decree No. 231/2001 extends the liability of entities to manslaughter and accidental actual or grievous bodily harm, committed by the parties referred to in Art. 5 of the Decree (i. e. persons who hold representation, administration or management functions at the entity, as well as by persons who exercise legal or de facto management and control over the entity, or even by persons subject to management or supervision by the parties indicated), in breach of the accident prevention and workplace health and safety regulations.

According to the current wording of the legislation, the occurrence of an accident at work, which results in the death of or actual or grievous bodily harm to an employee, may not only render the legal representative or party vested with accident prevention powers criminally liable (or, in any case, subject to criminal proceedings), but also render the entity administratively liable for not having adopted all the measures necessary for preventing and forestalling the offence.

Art. 25-septies takes into consideration crimes punished as unintentional ("*A crime is involuntary, or unintended, when the event, even if foreseen, was not intended by the perpetrator and occurs because of negligence, recklessness or incompetence, or through non-compliance with laws, regulations, orders or guidelines*", Art. 43 of the Italian Criminal Code). While the majority of the other crimes governed in the Decree consist in wilful acts, which thus presuppose awareness and intent on the part of the perpetrator as regards workplace safety, the grounds for the Company's liability lie in conduct that is involuntary, but characterised by negligence, recklessness or incompetence.

Lastly, Italian Legislative Decree No. 81 of 9 April 2008, as subsequently amended (Consolidated Law on workplace health and safety) reorganised the multiple legislative sources in effect in this field.

Art. 30 of Italian Legislative Decree No. 81/2008, in particular, lays down complex and structured regulations indicating the characteristics that Organisation and Management Models must possess in order to also produce their effects in the workplace health and safety sector. In particular, Art. 30 states that the adoption of the Organisation and Management Model, in order to be fully effective, must be accompanied by a company system that guarantees compliance with all legal obligations pertaining to: "a) compliance with legal technical/structural standards relating to equipment, plants, workplaces and chemical, physical and biological agents; b) risk assessment activities and development of the resulting prevention and protection measures; c) activities of an organisational nature, such as emergencies, first aid, contract management, periodic safety meetings, consultations with worker safety representatives; d) health supervision activities; e) worker information and training activities; f) monitoring activities with reference to compliance with workplace procedures and by the workers; g) acquisition of the documents and certificates required by law; h) periodic checks of the application and effectiveness of the procedures adopted".

The articles of law cited below are reproduced in the regulatory Appendix attached to this Model.

Manslaughter and actual or grievous bodily harm, caused in violation of accident prevention and workplace health and safety regulations (articles 589 and 590 of the Italian Criminal Code)[23]
Even if, from the perspective of the text, any party may be the perpetrator of the crime, for our purposes here and solely as regards the execution of the Company's activities, the principal recipient of the regulation in question is the employer, i.e. the holder of the employment relationship who, as such, is required to create and maintain all the conditions introduced to protect workers' health and safety.

Obviously, in cases where the employer has delegated its powers regarding the protection of workplace health and safety to one or more persons, they may also be considered perpetrators of the crime. In general, the crime in question may be committed by anyone who has held, ab initio, or adopted, including by means of a negotiating act (such as the aforementioned delegation, provided that, in such a case, it has been validly conferred), a position of guarantee with respect to the workers, i.e. anyone who has an obligation, ratified by law, to ensure that all workers can carry out their duties in maximum safety, based on measures that may actually be adopted in accordance with the current state of the art.

Bodily harm (Art. 590 of the Italian Criminal Code)
As for the commission of the crime in question, all the points made with regard to manslaughter apply. In this case, obviously, the event which constitutes the crime is not death, but bodily harm to a person: in fact, by limiting the focus to the scope of application of this Model, the only type of crime "of interest" is an accident (or illness) that results from an infringement of workplace accident prevention regulations and which causes bodily harm that may be qualified as "actual" or "grievous".

In accordance with Art. 583, bodily harm is **actual** if:
- the event causes an illness which endangers the victim's life, i.e. a disease or inability to perform ordinary activities that lasts for more than forty days;
- if the event causes the permanent weakening of a sense or an organ.

In accordance with the same regulation, bodily harm is **grievous** if the act causes:
- a certainly or probably incurable disease;
- the loss of a sense;
- the loss of a limb or a mutilation that makes the limb useless or the loss of use of an organ or the ability to reproduce, or a permanent and serious speech impediment;

disfigurement, or a permanent facial scar.

By virtue of this structure, the Company:
- issues procedures/orders aimed at defining formally the duties and responsibilities in relation to safety;
- monitors workplace accidents and regulates communication activity with INAIL, in line with legal provisions;
- monitors occupational diseases and regulates the communication activity of the respective data to the National Register for occupational diseases established at the INAIL database;
- adopts a procedure/internal order for organising preventive and periodic health checks;

[23] The articles of law cited above are reproduced in the regulatory Appendix attached to this Model.

- adopts a procedure/internal order for managing first aid, emergencies, evacuations and fire prevention;
- adopts procedures/orders for the administrative management of cases of accidents and occupational diseases.

As part of the clear definition of the specific functions in relation to workplace health and safety, the Company has identified the set of individuals engaged in the supervision activities and the implementation of the planned safety measures, granting a specific delegation in this regard, with the methods and limits indicated in Art 16 of Italian Legislative Decree 81/08.
In particular, the company Prevention and Protection System (PPS) is made up of:

- the Employer, identified by the Board of Directors as the figure having adequate organisational, decision-making and expenditure powers, in charge of coordinating all stakeholders and the respective activities under the remit of the PPS;
- the Delegated Manager, identified by way of a specific deed of delegation issued by the employer, granted responsibility for implementing some of the measures envisaged for the prevention and protection of the health and safety of workers;
- the Head of the Prevention and Protection Service (HPPS), appointed by the Employer subject to consulting with the Workers' Safety Representative (WSR).
  In DNWT, the HPPS is an external individual and the granting of the assignment and the respective acceptance by the latter is formalised in a specific contract;
- the Company Doctor in charge of guaranteeing compliance with the provisions on workplace safety;
- the Workers' Safety Representative (WSR), identified and designated by all Employees with methods compliant with the national collective labour agreement for the industry;
- the Supervisor, as a figure identified by the Employer within each organisational unit who, based upon the hierarchical powers functional to the nature of the assignment granted to him/her, supervises the working activity of the resources assigned to the same and guarantees that the directives received are implemented, checking their correct execution by workers and performing a functional power of initiative;
- the emergency and first aid officers, identified and designated by the Employer (or Employer's Delegate);

The overall and documented assessment of all risks to the health and safety of workers present within the organisation is carried out by the Employer, in collaboration with the members of the Prevention and Protection Service, and is formalised in the "*Risk Assessment Document at a certified date*", as required by the regulations in force in this regard; that document, as well as detailing the organisational structure in charge of preventing the crimes in question, identifies and assesses at a certified date the risks within the workplaces related to the protection of workplace health and safety, also assessing the potential hazards identified.

Any workplace accidents are reported by the Personnel Department to the Employer, who, in turn, informs the Supervisory Body pursuant to Italian Legislative Decree 231/01, also for the purposes of proposals of update to the Model and the subsequent *follow-up* on any additional measures adopted.

The Employer monitors the effectiveness and efficiency of the safety management system by way of periodic meetings, at least annually, at which the following persons attend, in addition to the Employer:

- The Head of the Prevention and Protection Service;

- The Company Doctor;
- The Workers' Safety Representative;

During those meetings, the following are assessed:
- the "*Risk Assessment Document*";
- the trend of accidents and occupational diseases and health supervision;
- the criteria of choice, the technical characteristics and the effectiveness of personal protective equipment;
- the information and training programmes of managers, supervisors and workers for the purposes of safety and health protection.

In accordance with Art. 41 of Italian Legislative Decree 81/08, the Company Doctor organises health supervision.

The Company constantly oversees the training level of employees on workplace safety, regularly planning information/training sessions aimed at all employees (including managers) on Italian Legislative Decree 81/08, as well as periodically updating the training of first aid officers, fire prevention offices and the WSR. Together with the "static" prevention and safety measures, DNWT constantly informs its workers on the risks in their working activities, training them on the measures suited to avoiding risks or to minimise them (implementing the necessary forms of personal protection).
With regard to activities supplied by providers of services based upon works contracts, the respective methods of managing and coordinating the works are formalised in specific contractual clauses, forming an integral part of the works contract, which expressly refer to the fulfilments indicated in Art. 26 of Italian Legislative Decree 81/08.

RISK AREAS

IDN's registered office is at Via Bistolfi no. 35 in Milan, where the offices, R&D laboratories and R&D workshop are located.

The Head of the Prevention and Protection Service, the Managers, the Company Doctor, the Workers' Safety Representatives - all in possession of the requirements envisaged by law - for both sites are formally appointed and the declarations of appointment are stored in specific archives.

In compliance with the provisions of articles 17 and 28 of Italian Legislative Decree no. 81/2008, the Company has drawn up a Risk Assessment Document (DVR - appended to this Model), which thoroughly analyses all health and safety risks inherent in company activities, providing details of the different types of activities and the various workplaces where the Company's activities are performed (with the content of the Document to be considered fully adopted in this Model).

The Company has also drafted an Assessment Document for certain Specific Risks, relating to risks from:
- Exposure to artificial optical radiation;
- Noise;
- Mechanical vibrations;
- Explosions;
- Electrical, magnetic and electromagnetic fields;

- Biological agents (e.g. COVID-19).

This document, in accordance with the regulatory provisions, identifies the prevention and protection measures introduced to safeguard workers and the programme of measures deemed suitable for guaranteeing improvement in safety conditions over time.
The Company's RADs have been drafted jointly between the Employer, the Prevention and Protection Service and the Company Doctor.

In referring to the approved RAD and the individual RAD for Specific Risks for further information, with reference to the "risk areas" at the different "workplaces", the following is specified:

a) Via Bistolfi no. 35, Milan - OFFICES
The administrative offices are at Via Bistolfi no. 35, Milan, along with the purchasing/production/planning and quality assurance offices.

Solely for the purposes at issue here (and, especially, with reference to the offences of manslaughter and serious or critical accidental injury), risk mapping has identified the presence of a risk. Moreover, said risk is extremely limited for workers performing 'Technical Staff' duties, who, when travelling abroad, may be required to operate in environments where the presence of airborne asbestos fibres cannot be excluded. The number of employees exposed to this risk is usually very low and, in any case, the workers in question have taken a specific training course on risks from asbestos and always use personal protective equipment when working in such environments.

With reference to ***fire risk***, the latter has been assessed in accordance with the provisions of existing regulations and the outcome of the assessment is to classify that risk as "low".

In accordance with the Italian Ministerial Decree of 10.03.1998, IDN has adopted a specific "Emergency and evacuation plan" for the facilities at Via Bistolfi no. 35, which is periodically subject to operating tests. In addition to the emergency evacuation procedures, this plan also identifies the fire prevention measures used and the existing active protection systems. It also governs the procedures for recording the periodic checks on safety measures (with identification of the staff responsible for safety, with particular reference to the fire prevention team) and the maintenance of the fire prevention systems and technological facilities.

Rules of conduct have also been outlined for personnel in the case of emergencies involving the immediate evacuation of the offices, containing the named indication of the personnel in charge of managing the emergency ("Conduct of personnel in the event of an emergency").

b) Via Bistolfi no. 35, Milan – R&D LABORATORY and R&D WORKSHOP

The R&D Laboratory constitutes the Company's centre for research activities in the industrial anodes segment.

In addition to normal office work, the work cycle envisages the following activities:

- Research & Development of electrodes, production of reduced-size prototypes and their characterisation through advanced analytical diagnostics and laboratory tests;
- Electrochemical and analytical services such as laboratory tests, electrochemical characterisation, instrumental and classic analytical diagnostics;

- Design of machines and facilities for the electrochemical industry, including operating tests on a suitably reduced scale and mechanical, electrical and thermal tests of components in the development phase;
- Mechanical processing for the construction of testing devices and the assembly of experimental components;
- Ordinary and extraordinary maintenance of equipment and apparatus.

Referring to the Risk Assessment Document, as well as the Specific Risk Assessment Documents in force, for all further details, following the *risk assessment* activities, the risk areas may be identified as follows:

- Noise (only within the Workshop Department);
- Ionising radiation;
- Artificial optical radiation (only in the Workshop Department and assessed as "medium risk");
- Use of compressed air;
- Use of specific work equipment;
- Mechanical vibrations (only in the Workshop Department);
- Low-frequency magnetic and electrical fields (only in the Workshop Department);
- Risk of explosion (risk present only in some laboratories and classed as "low");
- Manual handling of loads

With reference to ***chemical risk***, on the other hand, in view of the fact that the use of chemical substances may cause health risks if the chemicals are classed as hazardous and the conditions are met for possible interaction between such substances and employees while carrying out their duties (in the form of ingestion, contact with the skin or inhalation), the risk in question has been classed as low for safety and immaterial for health (for further details, see the "Technical assessment report on risks connected with exposure to hazardous chemical agents").

With reference to ***fire risk***, this was assessed in the light of legislation in force, and the outcome of the assessment classified such risk as "medium" (for the Workshop alone, however, the risk is considered "low") .

In this regard, see the details in the previous point as regards the content of the Site Emergency Plan (covering the entire facility at Via Bistolfi no. 35, including the R&D laboratories and the Workshop).

Some tasks in the production cycle face risks linked to the presence of **carcinogenic agents**. Since these are laboratory activities, any exposure will not be frequent but could change significantly over time. All employees responsible at any given time for the processing operations involved receive training through specific courses.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at those persons who, by regulatory provision or contractual deed, assume within the Company a position of guarantee in relation to workers (employer, managers, supervisors), for the precise purpose of guaranteeing and ensuring workplace health and safety during work. Furthermore, all IDN employees are considered to be intended recipients of this Model.

CODE OF CONDUCT

General code of conduct

The general principles aimed at preventing crimes of manslaughter and serious personal injury or grievous bodily harm, committed in violation of the accident prevention rules and protection of health at work are indicated below.

It is the Company's duty:

- to guarantee fulfilments in relation to the health and safety of workers in the workplace, assessing the choice of equipment present in the workplaces;
- to check that all planned prevention and protection measures are implemented, guaranteeing that risk situations are constantly monitored;
- to deal with updating the Risk Assessment Document in accordance with Art. 17 of Italian Legislative Decree no. 81/2008 in relation to organisational and production changes relevant to the safety of workers, to any reports by the Company Doctor or in the event of supervening legislative changes;
- to provide adequate and continuous information to employees with regard to the specific risks of the company in general and their specific duties in particular, on the consequences of those risks and on the prevention and protection measures adopted;
- in particular, in compliance with the provisions of the "*Onboarding Process*", which is binding for all Group Companies, the Human Resources Department must guarantee, with the collaboration of the Prevention and Protection Service, that each new recruit is informed and trained:
  - on the concepts of risk, damage, prevention and protection;
  - on the company's organisational structure in relation to safety and, in particular, the names of the employer, the head of the Prevention and Protection Service, the company doctor and the workers' safety representatives;
  - on the content of the evacuation and emergency plans;
  - on the specific risks linked to their job within the company, by the supervisors based upon the respective areas of responsibility (the Head of the Human Resources Area must ensure that a report is drawn up of the new recruit's training, which will then be added to the employee's file);
- to store in specific archives the documentation certifying the employee training activity;
- to deal with updating the existing procedures and operating instructions with a view to defining formally the duties and responsibilities on safety, also with reference to procedures for managing first aid, emergencies and evacuation and fire prevention procedures already existing;
- to ensure that all employees are adequately informed of the procedures in place for emergencies and evacuations;
- to ensure that employees working in the Workshop and Laboratories are adequately informed of the content of the Procedures and Operating Instructions in force and to ensure that the managers, supervisors and employees responsible for specific prevention and protection duties receive specific training;
- to ensure that all employees always have the personal protective equipment required according to the nature of the activity performed. A report must be drawn up of the delivery of PPE, which must be retained in a specific archive;
- to ensure that workers undergo medical examinations and tests, in accordance with the Health Supervision Programme currently in force, by the Company Doctor;

- to organise periodic meetings between the functions in charge, which may also be attended by the Supervisory Body, by convening meetings and respective minute-taking;
- to archive and store all documentation produced, also electronically or online, relating to the execution of the fulfilments carried out as part of the risk management processes in relation to the health and safety of employees as well as the respective control activity.

All Company employees, as well as external collaborators, are obliged to:

- in conducting their duties, comply with the rules and instructions imparted by the employer, by the managers and by the supervisors;
- comply scrupulously with the rules of law and, above all, the internal operating instructions on workplace safety;
- correctly use the machinery, equipment, tools, chemical substances present in the company;
- use the personal protective equipment recommended or made mandatory based upon the activity performed, and made available by the Company;
- attend training courses, when envisaged;
- undergo health checks planned for them in accordance with the deadlines set in the Health Supervision Programme by the Company Doctor;
- report to the persons in charge of compliance with the safety rules or, in any case, to the SB any potential hazard situation that occurs or that is currently ascertained or considered.

Code of Conduct in relation to specific Risk areas. Relations with contractors

The Company must:

- check that procedures are being correctly applied for the management of works contracts, aimed at all those involved in the choice of companies/freelancers assigned work to be performed on IDN premises or who provide assistance to such companies. This Procedure identifies the preparatory activities for the assignment of work, services and supplies, especially in terms of checking the technical and professional suitability of the contractor;
- draw up and update the Interference Risk Assessment Document (DUVRI), which indicates the measures adopted to eliminate and, where this is not possible, reduce 'interference risks' to a minimum;
- ensure that the DUVRI, adjusted as works, services and supplies develop, is always attached to the tender or works contract;
- provide detailed information to contractors regarding specific risks in the workplaces where they are required to operate and regarding the prevention and emergency measures adopted in relation to its activities;
- adopt measures aimed at eliminating interference risks between workers from the various companies involved in the execution of the overall works.

Risks from hazardous chemical substances

The employer is required to:

- provide adequate information to employees regarding the precautions to be adopted to avoid contact with aggressive chemicals;
- ensure that the safety sheets for the various products used are properly stored in a suitable archive;
- provide employees with personal protective equipment (masks for acid fumes, goggles, gloves) to protect the skin, eyes and mucous membranes during operations that may cause risks of inhalation or accidental contact with hazardous chemical substances;

- ensure that the collective protective equipment in the workplaces work correctly (eye wash stations, showers, etc.);
- use extractor systems located throughout the critical areas of the facilities;
- label all receptacles containing chemical agents in accordance with regulatory provisions;
- forbid the pouring of chemical products into containers that are not properly identified;
- forbid the consumption of food and drink during work activities;
- forbid the use of food containers to store reagents.

Fire risks

The Company must:

- appoint fire prevention, fire fighting and emergency management officers and ensure their training;
- remove anything that might jeopardise the correct operation and use of fire prevention systems.

Risks from biological agents

The RAD also includes the biological risk among the specific risks.
The protection of the mental and physical integrity of employees, also from biological risks to which they are exposed in performing their work activities, is a specific obligation for the employer.
Biological pollutants or bio-contaminants means a variety of microorganisms, such as: viruses, bacteria, fungi, yeasts, protozoa, insects, biological material deriving from them and material of plant origin.
Microorganisms have been broken down into 4 hazard classes, with increasing values from one to four and of
which the fourth, the most hazardous, refers to microorganisms that contain all four negative characteristics considered, namely a "*biological agent that can cause serious diseases in humans and constitutes a serious risk for workers and may present a high risk of spread among the community; effective prophylactic or therapeutic measures are not usually available*".
In this regard, as part of the activity carried out by IDN the main risk of biological nature is definitely represented by situations of declared pandemic.
In fact, there is no doubt that the relevant regulations require the employer to adopt a series of protocols and measures in its workplaces to avoid the spread of viruses between employees, all the more so if, as in the case of COVID-19, it concerns a highly dangerous biological agent.

If a pandemic or epidemiological crisis is declared by the national and/or international government institutions, IDN, with the assistance of the company doctor and the HPPS, constantly monitors any specific urgent measures, orders and regulations adopted by the institutions, in order to be aware at all times of the instructions and guidelines to be followed to combine the continuation of production activities with the guarantee of healthy and safe working conditions and methods.

During the continuing emergency situation, IDN adjusts to legislative requirements, along with the specific Protocols envisaged by the relevant regulations and implements the necessary measures, based upon the "*principle of maximum technologically feasible safety*", according to which the employer, aside from specific regulatory requirements, bases its conduct on aspects of the best science and experience, to ensure that workers are placed in a position to operate in absolute safety.

Some of the generic measures that may be implemented are, for example:

- regulate the methods of access to the company by employees, possibly performing a body temperature check (in compliance with existing rules on privacy) or excluding access to those who have recently been in contact with persons testing positive for COVID-19;

- identify entry, transit and exit procedures for external suppliers, by pre-defined methods, routes and timescales, so as to reduce any contact with staff working in the departments/offices involved;
- ensure the premises are cleaned daily and sanitised periodically, along with the rooms, workstations, changing rooms and common and rest areas;
- ensure employees have personal protective equipment and implement personal hygiene precaution measures, providing them, in relation to work requirements, with masks, gloves, goggles, overalls, ear protectors, gowns compliant with the requirements of the scientific and healthcare authorities, as well as suitable hand sanitising gel;
- restrict access to common spaces, including the company canteens, smoking areas and changing rooms, ensuring the rooms are constantly ventilated, requiring people to remain only for a limited prior in those rooms and to maintain a distance of 1 metre from other persons in those rooms;
- plan reorganisation measures of the company activities, encouraging the use of digital alternatives (as well as facilitating smart working for all those activities that can be carried out at home or remotely) that allow for conferences and work meetings to be attended remotely;
- limit travel to cases strictly necessary;
- guarantee a shift rota for production workers aimed at minimising contact and creating autonomous, separate and recognisable groups;
- establish a procedure for managing employees with Coronavirus symptoms, in order to isolate that person, to provide him/her with a protective mask and to notify the competent health authorities which will carry out the necessary further interventions.

During the continuing pandemic situation, IDN, as well as informing both its employees and anyone who enters the company of the anti-contagion measures adopted, also by affixing informative instructions at the entrance and in the most visible company locations, considers the mental-physical situation of employees, also through periods of interaction between them.

In order to ensure the implementation of and compliance with the cited measures, the company collaborates with the management body, the persons responsible for workplace safety (HPPS, WSR and Company Doctor primarily) and the heads of human resources, also by establishing a specific "Task Force" which can act as a point of reference for employees, if needed.

DUTIES OF THE SB

In relation to the duties of the employer and the other persons required to comply with and apply the rules on health and safety of workers in the workplace, the duties of the SB will be the following:

- to oversee the correct fulfilment of the duties of persons found in a position of guarantee with respect to the protection of the safety of workers;
- to verify, when delegating powers in relation to workplace safety, the effectiveness of the powers held by the delegate, also with particular reference to the power of expenditure;
- to receive and examine any report from workers or any other person in the Company.
- to carry out control activities, also randomly, in relation both to the existence of adequate workplace health and safety measures, and to compliance with the regulations on safety by workers.

The Supervisory Body has the power to perform specific checks, also as a result of reports received; the Body also has the right to access all company documentation available in the matter, with no obligation to provide prior notice.

The Company has also established, at the request of the Supervisory Body, information flows suitable to allow the latter to acquire useful information to monitor accidents, critical issues and information on any ascertained or presumed occupational diseases. The Supervisory Body, in carrying out the activities indicated above, may make use of all competent resources in relation to workplace safety in the company.

The Supervisory Body is also responsible for assessing the effective connection between the various entities involved in the control system in accordance with the '231' decree and the special regulations on workplace health and safety.
To that end, the HPPS sends a **half-yearly report** to the SB - and participates with the latter at meetings at least every six months - to ensure the Supervisory Body is fully informed on the area of safety.

In a pandemic situation, the role of the Supervisory Body is also significant as it must in fact promote the intensification of prompt reciprocal information flows with the Board of Directors and the other entities in charge of managing risk, as well as propose specific extraordinary checks on the preventive suitability of the workplace health and safety measures adopted.

During the continuing epidemiological crisis, IDN implements specific information flows and internal reporting to the Supervisory Body of all initiatives undertaken by the company to protect workers; information is sent with a suitable frequency, in view of a possible sudden evolution of the emergency situation, subject to the obligation to immediately report any major event.

CHAPTER 6

CYBER CRIMES

Italian Law no. 48 of 18.03.2008, entitled "Ratification and implementation of the Council of Europe Convention on Cybercrime, opened in Budapest on 23 November 2001, and regulations for adaptation of the Italian legal system", introduced significant amendments to the cybercime regulations, with the aim of adapting national legislation to the guidelines identified by the Council of Europe in the Budapest Convention of 2001.

In particular, Law no. 48/08 introduces Art. 24-bis to the corpus of Italian Legislative Decree no. 31/2001, which ratifies extension of the administrative liability of legal entities to the most serious cybercrimes provided for in the Italian Criminal Code, provided they are committed in the interests of the company or they procure an advantage for it.

The articles of law cited below are reproduced in the regulatory Appendix to this Model.

THE CYBERCRIMES IDENTIFIED IN ART. 24-BIS OF ITALIAN LEGISLATIVE DECREE No. 231/2001

Illegal access to a computer or electronic system (Art. 615-ter of the Italian Criminal Code)

This crime consists either in gaining illegal access to a protected system (computer or electronic), or remaining there against the express or tacit will of anyone expected to retain confidentiality of the data and programmes contained therein.

The definition of "computer system" is contained in Art. 1, letter a) of the Budapest Convention of 2001, where they are identified as "any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data".

A computer system is called an electronic system when the processor is remotely connected to other processors.

In the light of the wording of the incriminating rule of reference, in order to be significant for criminal purposes, the illegal access (or stay) must concern a computer system or electronic system "protected by security measures".

The concept of "security measures" may encompass all protection measures, which, when breached, can restrict access to the data and programmes contained in the system. They may include, for example, alphabetical or numerical access codes (e.g. passwords), as well as anthropometric data that may be detected by a suitable sensor, or physical protection measures (e.g. metal keys for starting up the processor).

Illegal possession and dissemination of access codes to computer systems or electronic systems (Art. 615-quater of the Italian Criminal Code)

The rule punishes a series of actions in preparation for (possible) commission of the crime of illegal access to a computer or electronic system protected by security measures; in particular, actions will be punished which consist in the illegal dissemination of access codes, usernames or, more generally, any means permitting access to a system, the confidentiality of which must be guaranteed.

The subject of the crime may therefore be:

- access codes (or usernames), to be entered on a keyboard or otherwise communicated to the processor;
- logical (e.g. passwords) and physical tools (such as keys);
- "suitable indications or instructions" for gaining illegal access to a system, or information that makes it possible to evade or neutralise the measures that protect the system from illegal access.

For the crime to occur, it is necessary for the perpetrator to have acted in order to "procure a benefit for him/herself or for others or to cause damage to others".

Dissemination of equipment, devices or computer programmes aimed at damaging or interrupting a computer or electronic system (Art. 615-quinquies of the Italian Criminal Code)

Art. 615-quinquies punishes conduct that consists in the creation and/or dissemination of equipment, devices or computer programmes able to compromise the functioning of a computer system or electronic system (typically involving the introduction and subsequent spread of viruses that may damage the computer data and programmes).

It is not essential for actual damage to have been caused to the system, as conduct simply in preparation for acts that have a negative impact on the correct functioning of the system is also subject to punishment.

Illegal interception, obstruction or interruption of computer or electronic communications (Art. 617-quater of the Italian Criminal Code)

The offence may consist either in using fraudulent means to intercept a computer or electronic communication during transmission, or preventing or interrupting it (e.g. by deviating a flow of data from one computer to another). It is also forbidden to reveal, using any means of public disclosure, all or part of the content of an intercepted communication.

The fraudulent connotation of the conduct presupposes that it consists in the circumvention of any systems for protecting an ongoing transmission (e.g. by decoding data transmitted in encrypted form or overcoming logical barriers introduced to protect the system receiving or sending the communication) or in making the illegal intrusion undetectable by third parties.

A typical example of computer communications are e-mail messages, also if sent to several recipients.

The installation of equipment intended to intercept, block or interrupt computer or electronic communications (Art. 617-quinquies of the Italian Criminal Code)

The rule seeks to suppress actions preparatory to the true interception of computer communications during transmission, by preventing the illegal installation of "equipment intended to intercept, block or interrupt" computer or electronic communications or those sent between multiple systems.

For example, this may mean equipment that enables illegal access to a communication in progress between two computer systems, by exploiting the telephone connection, or the interception and/or decoding of the data flow in transit.

Damage to computer and electronic systems (Art. 635-bis of the Italian Criminal Code)
Damage to computer information, data and programmes used by the state or another public body or public benefit entity (Art. 635-ter of the Italian Criminal Code).
The two regulations punish both damage to data and damage to computer programmes; the sole difference lies in the material subject of the conduct. In Art. 635-bis, this is composed of the data and programmes of 'others' (with this expression referring not only to the property of others, but also to property over which they have right of use, e.g. under a lease agreement), while in Art. 635-ter, it comprises data and computer programmes used by the state or another public entity or entity of public interest.

For the purposes relevant here, 'computer data' means "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function" (see Art. 1b) of the Brussels Convention of 2001).

A "computer programme", on the other hand, refers to the ordered set of instructions through which the processor is able to operate.

Damage to computer or electronic systems (Art. 635-quater of the Italian Criminal Code)
Damage to computer or electronic systems of public interest (Art. 635-quinquies of the Italian Criminal Code)
Neither of these cases of damage concerns individual documents, data or computer programmes, but rather "computer or electronic systems", of any type and size, which may be connected remotely to other computers.

As in the previous case, the two rules at issue differ in relation to the material subject of the conduct. In Art. 635-quater, this is composed of the systems of 'others' (with this expression referring not only to the property of others, but also to property over which they have right of use, e.g. under a lease agreement), while in Art. 635-quinquies, it comprises systems of public interest.

The attack may target either the system as a whole or one or more of its material components, such as the monitor, keyboard and all connected peripherals: any violent act committed against any one of these assets may potentially involve the entire computer system.

As regards the definition of "computer system", Art. 1 of the Budapest Convention defines this as "any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data".

Electronic documents (Art. 491-bis of the Italian Criminal Code)
This provision actually equates, solely for the purposes of determining the possible commission of crimes of falsification governed by the Italian Criminal Code, traditional and 'paper' documents (the regulation refers solely to public documents) to electronic documents (also public) that may be used as evidence.

According to Art. 1, letter p) of Italian Legislative Decree no. 82 of 07.03.2005, containing the Digital Administration Code, an electronic document is "the electronic representation of legally relevant documents, facts or data".

According to the current wording of the regulation, the falsification of an electronic document – in order to be significant for criminal purposes – must concern a document "that may be used in evidence".

Cyber fraud by a party providing electronic signature certification services (Art. 640-quinquies of the Italian Criminal Code)
This is a crime that cannot be committed by "anyone", but only by an "electronic signature certification service provider" or a provider of other related services. This therefore significantly limits the potential perpetrators of the crime.

Nevertheless, it should be emphasised that, according to the general rules as regards complicity in the commission of a crime, one cannot rule out (above all in cases where the "certifier" has acted to procure an advantage for others) a contribution from other parties (especially the party requesting the certificate) when these parties have contributed (perhaps even solely at psychological level) to commission of the crime.

RISK AREAS

IDN adopts a policy that is particularly attentive and strict with reference to the use by employees of the IT tools provided to them and, more generally, IT security.

It should be specified that it is prohibited within the company to use devices that increase the possibility of intercepting the communications of others.

That said, as the widespread use of IT tools is prevalent within the Company, the potential risk areas are all those that involve the use of information and/or electronic technologies and, in particular:

- management of the user profile and authentication process;
- management and protection of the workstation;
- management of company email accounts;
- management and control of external accesses;
- protection of the company networks;
- relationships with external parties by way of the IT system.

RECIPIENTS OF THE SPECIAL SECTION

Each operator possesses a personal area on the company server file. This special section is, therefore, directed at the shareholders, members of all corporate bodies and employees who use an IT tool and have access to the company network.

CODE OF CONDUCT

With regard to the use of systems, tools, documents or IT data, all those who operate on behalf of the Company are required to comply with the procedures for managing IT security and for using IT and electronic tools currently in force in IDN.

As part of the management of IT processes, the Company has adopted an articulated system of binding procedures for all Group companies and, more specifically:

- *Access Control;*
- *ICT Change Management;*
- *ICT Incident Manager;*
- *ICT Compliance.*

In turn, the "*IT devices and systems regulation*" regulates the use of IT devices and systems (telephones, email, shared folders, internet, etc.) by all personnel of the Italian companies of the De Nora Group and external collaborators to whom, for any reason, a company device has been provided. In particular, according to existing company rules:

- access to data resources in electronic format occurs only via computers protected by username and password;
- for each computer and communication system, the user ID must identify only one user. for each system access authorisation levels are established as necessary;
- passwords must always be encrypted and must not be stored in legible format in places where unauthorised people may discover and/or use them;
- devices and programmes must only be installed and updated by personnel instructed to do so;
- the servers are protected by corporate antivirus systems;
- any change of working status of employees within the Company (consultants, temporary or contracted) must be communicated immediately by the human resources department to the information system administrators involved;
- the Company exercises access control to the systems in protection of the integrity of the data which are kept on the computers and communication systems. The security manager and the network administrator may restrict or revoke any privilege for users; demand that the user deactivates or removes data, programmes or other system resources that may threaten these objectives; consider any other solution necessary to manage and protect the IT system;
- the network units are areas for sharing purely professional information and they may not be used, in any way, for other purposes.

That said, the recipients of this special section must:

- take care of the IT resources assigned to them (desktop or laptop personal computers), store them appropriately and use them exclusively to carry out work activity;
- promptly report any theft or damage;
- change the password immediately if there is any suspicion that it has been disclosed, intercepted or known by unauthorised persons;
- report any security incidents (also concerning attacks on the IT system by external hackers), making available all documentation relating to the incident.

The recipients of this special section are expressly prohibited from:

- leaving their workstation unattended for lengthy periods;

- communicating to others, beyond the permitted cases, their identification code (User ID/Username) and password for accessing the company network;
- transcribing on paper or memorising on magnetic medium their identification code (User ID/Username) and password for accessing the company network;
- accessing the company server folders without authorisation;
- procuring, reproducing, disseminating without authorisation access codes or means suitable to access a system protected by security measures;
- installing software (or even simple updates) on the personal computer and/or network servers without receiving express authorisation from an IT security coordinator;
- exploiting the weaknesses or deficiencies of the IT security system to damage systems or data, obtaining resources for which they do not have authorisation, removing resources from another user or having access to systems for which they do not have the necessary authorisations;
- using programmes and/or equipment and/or tools suitable to intercept, falsify or alter the content of IT communications and/or documents sent and/or received electronically as part of their duties;
- destroying, deteriorating, cancelling, altering information, data or IT programmes or others or even just endangering the integrity and availability of information, data or programmes used by the State or by another public entity or in any case of public interest;
- modifying, in the absence of prior authorisation of Company Management, the configuration of the personal computer used by the individual recipient;
- copying and holding beyond the permitted cases, even if only temporarily, files and documents of uncertain origin on magnetic and/or optical media and/or on the company personal computer;
- positioning on the company network, even if only temporarily, files and documents of uncertain origin that do not relate to the conduct of the work activity.

DUTIES OF THE SB

With regard to the prevention and supervision of cyber crimes, the duties of the SB will be the following:

- monitor to ensure that the measures to protect and store access codes, security keys and any other means suitable to allow access to the IT and electronic systems are established;
- to carry out any assessment considered appropriate on the individual risk operations;
- to analyse any report that is received in relation to possible violations of this Special Section or relating to the commission of illegal acts or even just "suspicious" acts, preparing a specific report to be sent to the Board of Directors and proposing, if necessary, the adoption of appropriate disciplinary measures;
- indicate to management any appropriate change and innovation in the procedures, to better prevent the risk of committing crimes.

CHAPTER 7

CRIMES AGAINST TRADE AND INDUSTRY AND IN RELATION TO COUNTERFEITING

Italian Law no. 99 of 23.07.2009 expanded the category of "predicate offences" provided for in Italian Legislative Decree no. 231/2001, by introducing the administrative liability of entities with reference to crimes connected with the counterfeiting of trademarks, designs and/or patents and to crimes against trade and industry.

Following this regulatory change, stricter legislation was introduced to protect industrial property, since civil law remedies (see Italian Legislative Decree no. 30 of 10.02.2005) were no longer considered sufficient in themselves to adequately tackle the phenomenon of counterfeiting.

Clearly, it was deemed appropriate to extend administrative liability to such crimes in order to protect patents (to the extent relevant here), i.e. one of the most costly company assets to obtain, in terms of human and financial resources used.

The Regulatory Appendix, attached to this Model, reiterates the legal articles taken into consideration by Italian Legislative Decree 231/2001 as regards crimes against trade and industry. Here below is a brief illustration of the sole crimes which may apply within the Company.

Counterfeiting, alteration or use of trademarks or logos or patents, models and designs (Art. 473 of the Italian Criminal Code)

Art. 473 of the Italian Criminal Code establishes two distinct cases: the first concerns the counterfeiting or alteration of "trademarks and logos" of industrial products or of "patents, designs or industrial models", while the second concerns the use of counterfeit or altered trademarks or logos or patents. The list should be considered compulsory.

Application of the first paragraph of the provision is limited, in accordance with prevailing case law, solely to registered trademarks. In order for a crime to have been committed, it is therefore necessary for the trademark to have been registered, since the Italian Intellectual Property Code stipulates that the provision will only be enforceable following registration.

Conversely, with reference to the second paragraph, it should be noted that, according to the most common case law interpretation, the regulation does not punish counterfeiting or alteration of the document in which the patent is granted, but rather the patented creation itself.

In order for the crime to have been committed, the current wording of the regulations requires that the perpetrator be merely aware of the existence of an industrial property right of another party ("… capable of knowing of the existence of the industrial property right").

In any case, the crime is necessarily deliberate in nature, insofar as the perpetrator must not only be aware and approve of the counterfeiting or alteration, but must also be aware that the trademark (or patent etc.) has been filed or registered.

Introduction into the country and trade of products with false markings (Art. 474 of the Italian Criminal Code)
The regulation establishes two distinct cases, the first of which (in paragraph 1) concerns solely the introduction into the country of industrial products with counterfeit or altered markings, while the second (paragraph 2) concerns various forms of conduct, including holding such products for sale, selling them or otherwise putting them into circulation.

"Introduction into the country" occurs when the falsely marked products or intellectual property have crossed the border.

"Holding for sale" occurs as soon as the perpetrator comes into possession of the falsely marked merchandise in order to sell it.

As regards "selling", it is not necessary for the agent to have offered the falsely marked merchandise or to have clearly displayed it. For example, simply having a stock of such products at the premises used for trading would be sufficient.

"Putting into circulation" encompasses all cases of putting falsely marked products placed on the market.

In its current wording, the crime (including all the forms of conduct listed in the two paragraphs) requires the agent to have acted "in order to gain a profit", which refers to the necessary presence of a profit-making purpose in the potentially criminal actions of the perpetrator.

Disturbed freedom of trade or industry (Art. 513 of the Italian Criminal Code)
This crime consists in using violence against property or fraudulent means to obstruct or disturb the exercise of trade or industry. The offence can be committed by anyone.

The prerequisite for this crime is that the act must not constitute a more serious crime; therefore, only generic acts against trade and industry are punished, in which a more serious offence cannot be identified (e.g. market rigging – Art. 501 of the Italian Criminal Code; sabotage – Art. 508 of the Italian Criminal Code; duress – Art. 610 of the Italian Criminal Code; unfair competition with threats or violence – Art. 513-bis of the Italian Criminal Code).

This is a 'dangerous' crime. It is therefore sufficient for the violence or fraudulent means to be fit for purpose, irrespective not only of the success of the criminal activity, but also of the actual disturbance to the exercise of trade or industry.

Unfair competition with threats or violence (Art. 513-bis of the Italian Criminal Code)
Unlike the crime referred to in Art. 513 of the Italian Criminal Code, this type of crime may only be committed by those who "exercise a commercial, industrial or in any event productive activity".

Typical conduct consists in acts of competition with violence or threat in the exercise of business activities against other companies operating in the same sector, i.e. in a situation of potential conflict. In this context, violence or threat should be understood as any violent or even merely intimidatory behaviour likely to prevent the competitor from making a free choice in exercising his or her business activities.

Fraud against national industries (Art. 514 of the Italian Criminal Code)
For the conduct described in the regulation to have occurred, it is sufficient to have marketed products with altered or counterfeit markings, when this causes harm to national industry, irrespective of compliance with laws on the protection of industrial property.

For the crime to have occurred, the conduct must have caused harm to national industry (understood as a reduction of business in Italy or abroad or the tarnishing of the good name of the national industry as an effect of unfair competition committed by whoever puts falsely marked products into circulation); as you might easily imagine, this is a material event of enormous proportions and extremely difficult to verify.

Fraud in the exercise of trade (Art. 515 of the Italian Criminal Code)
The conduct described here entails the delivery of products that differ in terms of origin, source, quantity or quality from what is described in the contract, irrespective of whether or not the perpetrator used particular expedients to mislead the buyer. Despite the use of the term "fraud", the presence of any manipulation, subterfuge or deception to the detriment of the purchaser lies outside the scope of the crime.

Fraud in the exercise of trade consists solely in the patently aware and deliberate unfair execution of the contract.

"Diversity of origin" refers to a different place of production, or a different product preparation system; "diversity of source", where not the same as diversity of origin, as is often the case, does not relate to the original place of production, but rather to the presence of an intermediary offering special guarantees of quality; "diversity of quantity" applies to weight, measurement or number; "diversity of quality", lastly, assumes an identical type of case but differing in essential qualities in relation to its usability, value or degree of conservation.

Sale of industrial products with false markings (Art. 517 of the Italian Criminal Code)
The prerequisite of the crime is the existence of names or trademarks that characterise the product, by identifying it and distinguishing it from others of the same type. The agent's exploitation is therefore by applying it to a similar product and in doing so misleading the consumer as regards it true source and quality.

The 'likelihood of confusion' in the logos or the false nature of their indications must be likely to mislead any purchaser as regards the product characteristics, according to the "average consumer" parameter.

This crime is secondary in nature, i.e. it only applies when the conduct does not constitute a more serious crime (as a rule, those referred to in articles 473 and 474 referred to above).

Manufacture and trade of goods created usurping industrial property rights (Art. 517-ter of the Italian Criminal Code)
This incriminating rule of reference, recently introduced, governs two independent crimes. Paragraph 1 covers the conduct of whoever manufactures, uses or applies products in infringement of an industrial property right; the second paragraph, on the other hand, punishes the conduct of anyone who, in order to gain a profit, imports and sells counterfeit goods.

This article, specifically the first paragraph, as in Art. 473 of the Italian Criminal Code, includes the aside "…*capable of knowing of the existence of the industrial property right*". This means that the manufacture or use of products protected by an industrial property right is punished only if the requirement of recognisability of industrial property rights to third parties is met.

RISK AREAS

Since IDN is particularly active in the research and development sector, "risk areas" may be considered those in which the activities are carried out likely to involve intellectual and/or industrial property rights of third parties. Of all the crimes envisaged in this section of the Model, therefore, the only ones that may potentially be considered a risk are those of "falsification of instruments or identification marks", especially those that concern patents, designs or industrial models.

In the Research and Development Department, IDN has a section specifically dedicated to intellectual property, which periodically conducts thorough scrutiny of the patent applications filed in sectors that may, in any way, concern the activities of the Company.

The abstracts of the patents deemed of interest are circulated to a distribution list, periodically updated when notified by the various function heads, which contains all the company functions concerned.

RECIPIENTS OF THE SPECIAL SECTION

Since these crimes involve, in particular, the Research & Development Department, as well as the production and commercial functions, this section of the Model is mainly aimed at those who, in various ways, are involved in procedures for implementation of the Company's technological assets.

CODE OF CONDUCT

Within the framework of intellectual property protection, the Company has adopted a system of procedures and operating protocols, binding on all Group Companies, under the responsibility of the IP Department, which governs intellectual property matters, specifically:

- *"Patent and Trademark Valuation";*
- *"Inventors' Reward and Recognition Program";*
- *"IP Main Processes";*
- *"IP Deliverables for R&D projects"*

In addition, the Company Code of Ethics lays down rules of conduct for the Corporate Bodies, Employees and Consultants, in order to prevent and impede criminal conduct that may constitute the type of crime of disturbed freedom of trade and industry and unfair competition with threats or violence.

In this regard, the Group Code of Ethics reiterates, in general, the obligation to operate in compliance with existing laws and professional ethics, and draws the attention of the Recipients to the opportunity to maintain in all situations conduct based upon the utmost correctness in relationships with third parties in general and with competitors in particular.
Furthermore, again in compliance with the Code of Ethics, it is prohibited for employees to use any information, documentation or data, and to manage the same via the company network drives, as well as on any electronic medium assigned to employees, other than data and information forming part of the Company's wealth of information.

Specifically, in order to prevent any risk of compromising the intellectual property rights of others, the following provisions must be complied with:

- at the time of recruitment, each new recruit must be informed of the relevant regulatory context and the general principles that govern the protection of intellectual property;
- the sheets relating to these informative discussions, containing a summary description of the topics covered and signed by the interested parties, must be kept in the personal file of the employee;
- all employees operating in the company functions concerned are required to participate, at least once, in a training session covering the main principles of the protection of intellectual property;
- the Intellectual Property office is required to periodically monitor patent applications made by third parties and identify registration requests that may be similar to the technologies employed by the company. Patent applications flagged as a possible source of present or future counterfeit risk are reported to the functions concerned;
- no new product or process will be produced, commissioned, offered for sale or marketed without a territorial search to verify that there are no valid patents held by other parties in the context in which the new product (or new process) is likely to lie;
- before filing any patent application, inventors are required to sign a declaration certifying that the list of inventors, in consideration of the claims, is accurate and complete;
- it is forbidden to disclose information to third parties concerning the technical, technological and commercial know-how of the Company, except in cases where such disclosure is requested by the judicial authorities, by a law or other regulatory provision or where it is expressly provided for in specific contractual agreements through which the counterparties have undertaken to use it exclusively for the purposes for which such information is sent and to uphold its confidentiality.

Relationships with customers

Relationships with customers are based upon principles of transparency, fairness and good faith and compliance with the agreed contractual terms.

The commercial terms are established by decision-making processes that can be reconstructed over time and are authorised exclusively by persons having suitable powers according to a system of delegations and powers of attorney coherent with the organisational and management responsibilities.

Operations relating to purchases and quality control of raw materials.

The function in charge of purchasing raw materials and semi-finished products:

- acquires information on the quality of the products, as well as qualitative indications and any product certifications, in order to ascertain that the same reflect the real characteristics of the product;
- ensures the systematic update of the contractual *standards* protecting industrial property coherent with evolutions of the legislation in force;
- enters, in the case of products not trademarked or patented by the supplier, clauses aimed at ensuring the commitment by the supplier to communicate without delay any disputes originating from third parties regarding the ownership of industrial property rights or logos, or disputes by other purchasers regarding the characteristics or logos of the goods supplied;
- interrupts the relationships with the supplier and recalls the item from production in the event of a clear infringement of intellectual property by the supplier itself and in the absence of an agreement with the third party allowing the Company legitimately to use the intellectual property of the latter.

Operations relating to the research and development of products

In relation to the research and development and sales and distribution activities of its products, the Company structures involved must:

a) verify, by the most appropriate methods, that the idea used in one or more parts of the product, the composition of the product, the production process used, the equipment used and the final product are not the reproduction of designs and models, inventions, patented or registered processes, national or foreign, owned by others. In the event of a suspected infringement, the Company completes all appropriate assessments to verify the infringement before marketing the product or making the patent application. The Supervisory Body is immediately informed of the event;
b) verify that all deeds, requests and communications aimed at filing patent and trademark registration applications are complete;
c) update the register of all patents owned by the Company in order to monitor the expiries of protection of the same and to renew them, where necessary;
d) identify the law firms and/or external consultants which support the Company in the activity of monitoring and protecting the trademarks and patents of the Company based upon requirements of professionalism and experience. The relationship with the external consultant is formalised in a contract that envisages specific clauses which indicate clear responsibilities in relation to the lack of compliance with this Special Section of the Company Model.

DUTIES OF THE SB

It is the duty of the SB:

- to constantly check the completeness and effectiveness of the provisions of this Special Section;
- to check compliance with the rules of conduct contained in this Special Section, by the respective recipients;
- to analyse any report that is received in relation to possible violations of this Special Section or relating to the commission of illegal acts or even just "suspicious" acts, preparing a specific report to be sent to the Board of Directors and proposing, if necessary, the adoption of appropriate disciplinary measures;
- indicate to management any appropriate change and innovation in the procedures, to better prevent the risk of committing crimes.

CHAPTER 8

CRIMES OF RECEIVING, LAUNDERING AND USING MONEY, GOODS OR GAINS OF ILLEGAL ORIGIN AND SELF-LAUNDERING

Through Italian Legislative Decree no. 231 of 21.11.2007 (known as the Anti-Money Laundering Decree), the legislator overhauled the framework of provisions aimed at combating money laundering and the financing of international terrorism, by reinforcing the mechanisms for preventing these crimes.

In particular, for our purposes, this decree - implementing Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as Directive 2006/70/EC laying down the related implementing measures - amended Italian Legislative Decree no. 231/2001, by introducing a new article (Art. 25-octies), which extended the scope of the administrative liability of entities to the commission of offences "pursuant to articles 648, 648-bis and 648-ter of the Italian Criminal Code".

Lastly, Italian Law no. 186 of 15.12.2014 included self-laundering among the predicate offences of administrative liability of legal entities (Art. 648-ter 1 of the Italian Criminal Code).

The articles of law cited below are reproduced in the regulatory Appendix to this Model.

Receiving (Art. 648 of the Italian Criminal Code)
Anyone who, with the aim of procuring unjust profit for themselves or others, receives or conceals money (but not only money) or in any case intervenes in the purchase, receipt or concealment of said money, is committing the crime of receiving.

For the crime to have been committed, the property or money received must be of illegal origin. The concept of "origin" encompasses everything connected with a criminal act, i.e. the profit, price, product of the crime and anything else used in its commission.

'Anyone' can commit this crime, except for the perpetrator or anyone who contributed to the predicate offence. In other words, a party guilty of the predicate offence can never also be charged with receiving.

Money laundering (Art. 648-bis of the Italian Criminal Code)
The crime of money laundering is committed by anyone who either: 1) replaces or 2) transfers money, assets or other benefits derived from a deliberate crime or, more generally, 3) carries out transactions on such assets that prevent the identification of the illegal source.

Given the specific wording of the regulation – which punishes "any transaction" capable of hindering the identification of the origin of the money – any conduct that might prevent the identification of the illegal source of money or other assets will constitute conduct that is relevant for the purposes of Art. 648-bis of the Italian Criminal Code.

'Anyone' might be a potential perpetrator of the crime, with the exception (as in the case of receiving) of anyone who has taken part, as participant, in the crime which was the source of the money, assets or other benefits gained from the crime. In other words, if the money laundering acts are committed by one of the participants in the predicate offence, they are considered ineligible for punishment since they represent the natural continuation of the criminal activity, aimed at retaining the profit derived from it.

Use of money, goods or other gains of illegal origin (Art. 648 ter of the Italian Criminal Code)
The conduct at issue consists in using, in economic or financial activities, i.e. in any sector used to generate profits, money, assets or other utilities of illegal origin (and precisely the proceeds of a crime). Through this regulatory provision, the legislator sought to underline the independent criminal significance of reusing illegal resources in production sectors, and especially in the finance, trade and industry sectors.

The perpetrator of the crime may be anyone who reuses illegal capital, aware of the criminal origin of the goods and perpetration of the crime, provided that – as in previous cases – they have not contributed to commission of the predicate offence.

Self-laundering (Art. 648-ter 1 of the Italian Criminal Code)
The crime of self-laundering punishes anyone who - having previously committed (or contributed to committing) any intentional crime - uses, replaces or transfers in economic, financial, business or speculative activities, money, assets or other gains originating from the commission of that crime, so as to hinder the effective identification of their illegal origin.

Unlike the offences of receiving, money laundering and reusing indicated above, a perpetrator of the crime of self-laundering can only be the same person perpetrating the offence that generated the illegal cash flow.

RISK AREAS
The investigations carried out during the "risk mapping" have identified as risk areas all those in which incoming and/or outgoing cash flows are generated.

In particular, the following company functions are at risk:
- negotiation and stipulation of supply contracts;
- purchase of goods and services;
- search, selection, approval and monitoring of suppliers;
- intercompany relationships;
- finance and treasury management;
- management of ordinary and extraordinary transactions;
- general accounting, financial statements and other corporate communications;
- relationships with the financial administration;
- search, selection and remuneration of personnel;
- management of gifts and entertaining expenses.

The list is obviously subject to changes and additions; if this becomes necessary, additional risk areas will be identified, with consequent preparation of specific rules of conduct and respective procedures.

In such cases, the SB is responsible for proposing to the Board of Directors any appropriate intervention on the text of the previous Special Section. The Board of Directors itself may also take similar initiatives autonomously.

The general principles of control established by the Company with the aim of preventing the commission of the crimes indicated in this Special Section are aimed at guaranteeing:

- the regularity of the sales and distribution cycle, so that every receipt occurs via traceable instruments (bank transfers, cash orders, promissory notes, cheques), as the use of cash or other similar payment instruments is prohibited;
- the regularity of the purchasing cycle, so that every payment occurs via similarly traceable instruments, as the use of cash or other similar payment instruments is prohibited;
- the appropriateness of payments or expenses reimbursements, remuneration, discounts, credit notes is adequately justified as part of the contractual relationships of reference;
- the existence of a regularity check of financial transactions;
- the existence of formal and substantial controls on company cash flows, with reference to receipts/payments from/to third parties or other Group companies;
- the complete traceability of data relating to cash flows incoming and outgoing from/to third parties or other Group companies.

As part of the management of procurement processes of goods and services used to create the end product, the Company has adopted a system of procedures, binding for all Group companies, aimed at regulating aspects concerning the purchase of goods and services as well as the selection and approval of suppliers and, more precisely:

- *Vendor Master Data Management;*
- *Procurement of Common Items;*
- *Organisational Document System;*
- *Material Master Data Rules;*
- *Titanium Scraps Management;*
- *Vendor Management;*
- *Planning and Procurement of Strategic Items;*
- *Vendor evaluation;*
- *Vendor Qualifications;*
- *Business Card Management.*

Payments are made according to the methods established in the "Treasury provisions for the payment of Italian/Foreign suppliers" of the De Nora Group.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at all managers, directors and employees of IDN who operate in the risk areas, as specified above.

The rules of conduct envisaged therein are also extended to and must be respected by external collaborators and commercial parties, who, as envisaged by the General Part of the Model, must also be made aware of its content.

CODE OF CONDUCT

This special section is aimed at indicating to the Recipients, to the extent to which they may be involved in carrying out the activities in the risk areas, the procedural rules and codes of conduct that may prevent and impede the occurrence of crimes against property identified by the Decree.

The Recipients of the Model are expressly obliged:

- to refrain from conduct that may constitute the aforementioned crimes of receiving, laundering, reusing and self-laundering, or from conduct that, although not actually constituting in itself a type of crime falling among those considered above, may facilitate their commission;
- to behave correctly, transparently and collaboratively, in compliance with the rules of law and internal company procedures, in all activities aimed at the administrative management of suppliers/customers/commercial partners, domestic or foreign;
- in particular, the commercial and professional reliability of suppliers and commercial/financial partners must always be verified based upon some significant indicators (e.g. public prejudicial data - protests, insolvency proceedings – or acquisition of commercial information on the company, the shareholders and the directors by way of specialist companies; price amount disproportionate to average market values);
- not to hold commercial relationships with persons (natural or legal) known to belong to criminal organisations or in any case operating outside of the law such as, by way of example but without limitation, persons linked to money laundering;
- to identify and register the data of natural or legal persons with which the company enters into purchase contracts necessary to develop the sales network, also abroad, and check that those persons are not based in or do not have their residence in or any link with countries considered uncooperative by the Financial Action Task Force (FATF); if the counterparties indicated in this area are in any way linked to one of those countries, the respective decisions must obtain the express authorisation of the Chief Executive Officer, having heard from the SB;
- not to use anonymous instruments to complete transactions transferring significant amounts;
- to check the regularity of the payments, with reference to the full matching of recipients/payers to counterparties actually involved in the transactions;
- to check the economic fairness of investments made with third parties;
- to perform formal and substantial checks of the company cash flows, with reference to payments to third parties and intercompany payments/transactions; those checks must take account of the registered office of the counterparties (e.g. tax havens, countries at risk of terrorism, etc.), credit institutions used (location of banks involved in the transactions) and any corporate schemes and fiduciary structures used for any extraordinary operations;
- to check the level of adjustment of the Group companies to the preparation of adequate anti-money laundering controls.

DUTIES OF THE SB

The recent regulations identified by Italian Legislative Decree no. 231/2007 imposes a specific anti-money laundering monitoring obligation on corporate bodies tasked with management control (also including the SB).

In particular, Art. 52, paragraph 1, of the aforementioned legislative decree imposes an obligation on the SB, the Board of Statutory Auditors, the supervisory committee and the management control committee to monitor satisfaction of the provisions contained in the new anti-money laundering decree.

These parties must:

- inform the Supervisory Authority for the sector, without delay, of all acts or events of which they become aware during the exercise of their duties, which could constitute a violation of any measures issued by the Supervisory Authority regarding the procedures for complying with customer due diligence obligations, the organisation, registration, procedures and internal controls aimed at preventing the use of intermediaries and other parties that carry out financial activities for the purposes of money laundering or the financing of terrorism;
- inform the owner of the business, or his/her legal representative or appointee, without delay of any infringements of the "suspicious transactions" legislation pursuant to Art. 41 of Italian Legislative Decree no. 231/2007;
- inform the Italian Ministry of Economy and Finance, within thirty days, of any infringements of the legislation in terms of limits on the circulation of cash and bearer securities of which it becomes aware (Art. 49 of Italian Legislative Decree no. 231 of 2007);
- inform the UIF (Financial Intelligence Unit), within thirty days, of infringements of provisions on registration obligations pursuant to Art. 36 of Italian Legislative Decree no. 231/2007.
- In addition to the aforementioned obligations, the SB is required:
- to check constantly the completeness and effectiveness of the provisions of this Special Section;
- to carry out any assessment considered appropriate on the individual risk operations;
- to indicate to management any appropriate change and innovation in company procedures, to better prevent the risk of committing crimes.
- to ascertain any infringement of this special section and propose the opening of any disciplinary proceedings.

CHAPTER 9

CRIMES IN RELATION TO THE ENVIRONMENT

After an initial extension of the administrative liability of legal entities to environmental crimes pursuant to Italian Legislative Decree no. 121 of 07.07.2011, "*Implementation of Directive 2008/99/EC on protection of the environment through criminal law, as well as Directive 2009/123/EC amending Directive 2005/35/EC on ship-source pollution and on the introduction of penalties for infringements*", Italian Law no. 68 of 22 May 2015 recently expanded the catalogue of environmental offences significant under Italian Legislative Decree 231/2001.

In the aforementioned Directive, the European Parliament highlighted how the use of criminal sanctions is an essential measure to combat environmental infringements, and required Member States to adopt effective, proportionate and dissuasive criminal penalties. There is also an obligation to extend them to the legal entities in whose interests or benefit the crimes have been committed.

The key new feature introduced by Italian Legislative Decree no. 121/2011 is the inclusion of certain environmental crimes among the predicate offences relating to administrative liability of entities referred to in Italian Legislative Decree 231/2001 (now contained in Art. 25-undecies)

In consideration of the fact that, among the offences considered by Art. 25-undecies, there is conduct that may be punished even if they prove harmless to the environment and to health (as in cases where there is no authorisation for the collection, transport and disposal of waste, etc.), it is clear that the topic of environmental crimes is particularly delicate and requires the company to make greater efforts in terms of the organisation and control of company activities.

The Regulatory Appendix, attached to this Model, reproduces the text of all the environmental crimes taken into consideration in Italian Legislative Decree 231/2001.

Here below is a brief illustration of the sole crimes which may apply within the Company.

Environmental pollution (Art. 452-bis of the Italian Criminal Code)

The crime of environmental pollution punishes anyone who compromises or causes significant and measurable damage to:

1) water or the air, or extensive or significant parts of the soil or subsoil;
2) an ecosystem, biodiversity (including agricultural biodiversity), flora or fauna.

The crime may be committed using any means, including through mere omission (in all cases where regulatory sources or specific provisions in individual authorisations require specific parties to prevent environmental pollution).

The only pollution significant for criminal law purposes is that caused 'illegally', i.e. which results from breaches of the law or the provisions contained in the permits.

Such cases are punished as wilful acts; this therefore presupposes conscious and deliberate infringement of the sector regulations or the provisions contained in the authorisations, as well as awareness that the perpetrator's actions compromise or damage environmental matrices.

Environmental disaster (Art. 452-quater of the Italian Criminal Code)
This regulation targets anyone who causes an "environmental disaster", an event which must involve one of the following:

1) irreversible alteration in the equilibrium of an ecosystem;
2) alteration of an ecosystem, the elimination of which is particularly costly and can only be achieved through exceptional measures;
3) threat to public safety caused by the significance of the event in terms of the extent of the degradation or its harmful effects or the number of persons injured or exposed to danger.

In this case too, as in the case of environmental pollution, the conduct described is punished to the extent that it is carried out 'unlawfully' (on this point, see the clarifications with reference to Art. 452-bis of the Italian Criminal Code).

The crimeis only punished if committed with wilful intent (unintentional crimes are covered and punished under Art. 452-quinquies of the Italian Criminal Code).

Unintentional crimes against the environment (Art. 452-quinquies of the Italian Criminal Code)
Art. 452-quinquies punishes conduct involving environmental pollution and disaster even if committed unintentionally, but the penalty is reduced (by one-third to two-thirds).

If commission of the above-mentioned crimes gives rise solely to the danger of environmental pollution or disaster (but they do not actually occur), the penalty will be further reduced by a third.

Conspiracy to commit environmental crimes (Art. 452-octies of the Italian Criminal Code)
Art. 452-octies introduces two new aggravating circumstances, increasing the penalty by up to one-third for crimes of conspiracy and mafia-like conspiracy, if aimed respectively at committing any one of the new environmental crimes or in any case at acquiring management or control of environment-related business activities.

unauthorised waste management activities (Art. 256, paragraphs 1, 3, 5 and 6, of Italian Legislative Decree no. 152/2006)
Before considering the merits of individual waste-related crimes, a brief mention should be made of exactly what waste is, from a technical/legal perspective.

Art. 183, paragraph 1, letter a) of the Consolidated Environmental Law defines 'waste' as "any substance or item which the owner disposes of or decides or is obliged to dispose of".

Annex D of Italian Legislative Decree no. 152/2006 contains a long list of waste, each marked with a six-digit code (EWC), and, where classed as hazardous, by an asterisk.

The classification of a substance as waste in the list in Annex D is of circumstantial value, which will be confirmed or refuted in the concrete circumstances of its actual use or function. Attention must therefore be given not only to the type of substance under discussion as waste, but also and especially its objective earmarking for dumping or disposal or, in any case, the decision of the producer of said waste to dispose of it or any legal obligation to do so.

The list of hazardous waste, however, is closed and fixed, unlike that of non-hazardous waste. The hazardous nature of a substance actually depends on objective characteristics (flammability, carcinogenicity, toxicity, etc.), which can be recognised and classified ex ante, irrespective of decisions of the holder.

Associating a substance with the concept of waste entails a series of obligations for the producers: to obtain prior authorisation or, in other cases, to register or report waste management activities (collection, transport, storage, disposal, recycling, etc.) to public bodies and entities; annotation in loading and unloading registers, on suitable forms in the case of transport, etc.

The aim is to ensure that the waste lifecycle is always traced from the time of its production until its disposal or recycling, so as to prevent waste management abuse or at least to be able to trace the perpetrators of any crimes ex post.

Art. 256, paragraph 1 renderes waste management activity a crime in the absence, depending on the case, of authorisation, registration or communication as required by the relevant administrative regulations. This is a crime involving abstract danger and is 'formal' in nature, with the legislator punishing the exercise of activities over and beyond prior controls by public administration, regardless of whether or not the activities are actually carried out in compliance with environmental regulations.

In case law, the absence of a permit is considered equivalent to its expiry or suspension (e.g. through failure to pay the related fees).

If the waste processed is hazardous, this is considered an aggravating circumstance.

Art. 256, paragraph 3, in turn, punishes anyone who implements or manages unauthorised landfill. “Implementation” means, in particular, the equipping of an area used as a landfill site: it therefore presupposes a de facto situation (earthworks, levelling, access roads) which makes the site usable as a deposit.

A "landfill" must be considered a site for the accumulation of waste which, due to its characteristics (nature, quantity, heterogeneity, geographic location, etc.), is not collected for assignment, within the allotted time frames, of one or more uses in accordance with law and which entail ongoing degradation of the land on which it is located.

An authorised landfill may also be illegal if a part of it is unlawfully used for storing waste other than that authorised, or if it is piled in an area different from that authorised, with the location being one of the characteristics assessed at the time of authorisation.

Art. 25-undecies of Italian Legislative Decree no. 231/2011 also makes express reference to Art. 256, paragraph 5 of the Consolidated Environmental Law, which punishes the mixing of waste of different hazardous characteristics or hazardous waste with non-hazardous waste. It is important to remember that prohibited mixing also includes the dilution of hazardous substances.

Site reclamation (Art. 257, paragraphs 1 and 2, of Italian Legislative Decree no. 152/2006)
The crime referred to in Art. 257 of the Consolidated Environmental Law (i.e. the crime of failure to reclaim a site) can only be committed by a party who "causes pollution of the soil, subsoil, surface water and groundwater".

In essence, only the party responsible for the polluting act may therefore be punished for failure to reclaim a site; the crime thus cannot be committed by a third party unconnected with the environmental contamination of the site.

This is because the party responsible for the polluting conduct has a personal obligation to eliminate the consequences of his/her actions. There can be no obligation, for example, for whoever was only able to use the area at a later date and made no causal contribution to the environmental pollution.

According to the wording of Art. 257 of the Consolidated Environmental Law, the crime occurs in relation to the person responsible for the pollution "if they fail to reclaim the area in compliance with the project approved by the competent authority as part of the proceedings indicated in Art. 242 et seq.".

For the crime to have occurred, therefore, the risk concentration threshold has to have been exceeded and the reclamation project approved, as detailed in Art. 242 et seq. of the Consolidated Environmental Law.

The commission of the crime must therefore incorporate the adoption of the reclamation project in accordance with the timescales and procedural guidelines noted in the aforementioned Art. 242.

Failure by the party that caused the pollution to notify the competent authorities of the existence of an event that might potentially contaminate the site is also a criminal offence.

Paragraph 2 of the regulation on this crime envisages an aggravating circumstance in cases where the pollution is caused by hazardous substances.

Violation of obligations to communicate and keep mandatory records and forms (Art. 258, paragraph 4, second sentence of Italian Legislative Decree 152/2006)
This provision punishes, with the penalties envisaged for the crime of ideological falsification of the private entity in a public act (namely with imprisonment of up to two years), the false indication in the analysis certificate of the nature, composition and chemical-physical characteristics of the waste as well as the related use during transportation.

Illegal trafficking of waste (Art. 259, paragraph 1, of Italian Legislative Decree 152/2006)
For the concept of "waste", see the points illustrated in Art. 256 of the Consolidated Environmental Law.

This case applies solely to cross-border shipments (i.e. from the country where the producer is located to another country), notwithstanding the reference to EEC Regulation no. 259 of 01.02.1993 (repealed and replaced by no. 1013/06), executed by parties who perform these activities professionally.

In accordance with Regulation (EC) no. 1013/06 (which, as mentioned previously, repealed Regulation 259/93 indicatedin the legislation), an "illegal shipment" is any shipment of waste effected:

- without prior notification to all competent authorities concerned pursuant to the regulation (Art. 2 no. 35, letter a));
- without the consent of the competent authorities concerned pursuant to the regulation (Art. 2, no. 35, letter b));
- with consent obtained from the competent authorities concerned through falsification, misrepresentation or fraud (Art. 2, no. 35, letter c));
- in a manner not materially specified in the notification or transport documents (Art. 2, no. 35, letter d));
- in a mannerresulting in recycling or disposal in contravention of EU or international regulations (Art. 2, no. 35, letter e));
- contrary to some articles of the regulation expressly referred to therein (Art. 2, no. 35, letter f)).

The penalty will be increased (by up to one-third) in the case of shipping of hazardous waste.

Activities organised for the illegal trafficking of waste (Art. 260 of Italian Legislative Decree 152/2006)
For the concept of "waste", see the points illustrated in Art. 256 of the Consolidated Environmental Law.

This represents the most serious offence as regards environmental crimes referred to in Decree no. 231/2001, which is already clear insofar as it is considered a crime rather than an infringement. Since this is a crime, it can only be punished as a deliberate act and constitutes a prerequisite for the application of a prohibitive sanction, in cases where the court believes that the entity was established for the sole purpose of committing the crime.

In essence, it is a sort of "criminal conspiracy" aimed at the illegal processing of waste, something that might involve all parties with a role in waste management, including the producer where he/she is aware, for example, of the infringements committed by the transport or disposal operator.

It is necessary for resources and continual, organised activities to have been arranged, an element which presupposes the creation of a business structure, even if only rudimentary, within which several people normally operate. The decisive factor in determining whether this crime has been committed is that each perpetrator must be aware that he/she is making a contribution that enhances the stability and continuity of the organised activities, with a view to obtaining unjust profit.

Computer system to monitor waste traceability (Art. 260-bis, paragraphs 6, 7 and 8, of Italian Legislative Decree 152/2006)
For the concept of "waste", see the points illustrated in Art. 256 of the Consolidated Environmental Law.

The need to reliably trace the path of the waste, so as to always be able to reconstruct its history and movements to the benefit of the bodies tasked with monitoring and repression, led the legislator to build a structured computer system to monitor waste traceability, entitled SISTRI, entrusted to the Carabinieri environmental protection force.

Some categories of waste managers are obliged to adopt a computer system which, once fully operational, will enable real-time verification of data relating to the waste produced, transported and subject to the various management operations. In particular, entities and companies that produce hazardous waste are obliged to adopt the SISTRI (Art. 188-ter of the Consolidated Environmental Law).

Art. 188, paragraph 1, of the Consolidated Environmental Law stipulates that the initial producer shall remain responsible for the entire waste processing chain, and therefore for handovers to third parties (for transport, recycling, disposal, etc.), except and "other than accomplices in the illegal act and the provisions of Regulation (EC) no. 1013/2006, where the initial producer, producer and holder are registered and have satisfied the obligations of the waste traceability monitoring system (SISTRI) pursuant to Art. 188-bis, paragraph 2, letter a)", in which case, liability will be limited to the spheres of competence stipulated by that system (Art. 188, paragraph 2, of the Consolidated Environmental Law).

In other words, there cannot be any illegality (administrative and criminal) with respect to the actions of others entailing illegal waste disposal or management, where the producer – registered on the SISTRI – complies with their electronic obligations.

Art. 260-bis of the Consolidated Environmental Law establishes a range of administrative crimes applicable to parties obliged to register on the SISTRI who fail to comply with the various provisions it imposes.

There are only certain acts subject to criminal penalties, however, and it is precisely these that are taken into consideration by Italian Legislative Decree no. 231/2001:

- that of a transporter who fails to accompany the transport of hazardous waste with a paper copy of the SISTRI-HANDLING AREA sheet and, where necessary, based on legislation in force, with a copy of the analytical certificate identifying the characteristics of the waste;
- that of anyone who, during transport, uses a waste analysis certificate containing false indications regarding the nature, composition and chemical/physical characteristics of the waste transported;
- that of a transporter who accompanies the transport of waste with a fraudulently altered copy of the SISTRI-HANDLING AREA sheet.

RISK AREAS

With reference to environmental crimes, the Company's risk areas are focused solely on waste.

In particular, hazardous and non-hazardous waste is produced at the R&D laboratory. The Company uses only authorised intermediaries which deal with the transportation and subsequent disposal phases, using, in turn, companies having the necessary authorisations required by the relevant regulations on waste management (copy of all authorisations of companies involved remains stored at the Company).

In any case, the risk of accidental pollution of the soil, subsoil, surface waters or underground waters cannot be excluded, meaning the Company will be obliged to perform reclamation of the site.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at all managers, directors and employees of IDN who operate in the risk areas, as specified above.

The rules of conduct envisaged therein are also extended to and must be complied with by external collaborators and commercial parties, who, as envisaged by the General Part of the Model, must also be made aware of its content.

CODE OF CONDUCT

This special section is aimed at indicating to the Recipients, to the extent to which they may be involved in carrying out the activities in the risk areas, the procedural rules and codes of conduct that may prevent and impede the occurrence of crimes against property identified by the Decree.

The Recipients of the Model are expressly obliged:

- to refrain from conduct that may constitute the aforementioned crimes in relation to the environment, or from conduct that, although not actually constituting in itself types of crime falling among those considered above, may facilitate their commission;
- to behave correctly, transparently and collaboratively, in compliance with the rules of law and internal company procedures, in all activities aimed at managing water discharges, waste and atmospheric emissions;

In particular, the Recipients of the Model are obliged to comply with the following rules of conduct:

- if the Company, in its capacity as a producer of waste (both hazardous and non-hazardous), does not carry out self-disposal or the delivery of waste to entities that manage said public service, it is obliged to ascertain that the companies to which it delivers the waste for disposal have the necessary authorisations for each of the relevant activities (transportation, temporary storage, disposal);
- a copy of the authorisations of each supplier (intermediary, transporter, disposal agent) must be stored in the company archives;
- when an event occurs, deliberate or accidental, that is likely to contaminate the soil, subsoil or surface and underground waters, the Company must immediately inform the competent authorities in accordance with Art. 242 of the Consolidated Environment Law;
- the waste analyses provided for the disposal (hazardous and non-hazardous) must be carried out at least half-yearly for hazardous waste and annually for non-hazardous waste;
- indications on the nature, composition and chemical-physical characteristics of the waste recorded by analysis certificates must always be true;
- waste analysis reports must remain stored in the Company archives, by the Secretariat of the R&D Department for the Milan laboratories, and kept available for checks by the competent authority:
- copies held by the producing Company of the transportation forms of waste transported for disposal must remain stored in the Company archives, under the responsibility Secretariat of the R&D Department for the Milan laboratories, and kept available for checks by the competent authority;
- waste awaiting disposal must be deposited in clearly delimited areas marked by specific identification signs and each set of waste, in turn, must be identified correctly according to its type;
- in areas where hazardous waste is deposited, marked by specific signage, access is prohibited to unauthorised persons;
- the waste must remain deposited inside the production site for the time strictly necessary to provide it to the transporter for subsequent disposal;
- on an annual basis, the Company, under the responsibility of the Secretariat of the R&D Department for the Milan laboratories must send the Single Environmental Declaration Model (MUD) to the Chamber of Commerce;
- copies of the MUD sent must remain stored in the Company archives and kept available for checks by the competent authority:

- the Company is required to allow the production plant to be accessed by the competent authority for checks and to provide all information requested;

DUTIES OF THE SB

In relation to the duties of the employer and the other persons required to comply with and apply the rules on the environment, the duties of the SB will be the following:

- to oversee the correct fulfilment of the duties of persons found in a position of guarantee with respect to the protection of the environment;
- to receive and examine any report from workers or any other person in the Company;
- to carry out control activities, also randomly, in relation both to the existence of adequate workplace health and safety measures, and to compliance with the regulations on safety by workers.

CHAPTER 10

INCITEMENT TO NOT TESTIFY OR TO BEAR FALSE WITNESS

Italian Law no. 116 of 3 August 2009, "Ratification and implementation of the United Nations Convention against Corruption" introduced Art. 25-*decies* to Italian Legislative Decree 231/2001, whereby entities may also be liable in relation to the crime indicated in Art. 377-bis of the Italian Criminal Code, namely "incitement not to testify or to bear false witness".

The regulation seeks to protect the correct execution of activities of the judicial authorities and the determination of the truth in criminal proceedings. To this end, punishment is established for incitement not to testify or to bear false witness, committed with respect to a person called upon to report to the legal authorities and who has the right to silence (the textbook example is a line manager who threatens a subordinate, forcing him/her to make reticent or false statements to judicial authorities).

The generic reference to "judicial authorities" encompasses both the courts and the public prosecutor.

The "victim" of the crime must be a party who, as stipulated in the text of the regulation, may exercise the right to silence. The reference is therefore clearly to suspects and the accused in a criminal trial (or associated proceedings), to whom the law specifically grants the right to silence.

Lastly, for the crime to have been committed, it is necessary for the "threatened" party to actually refuse to testify or to bear false witness.

The article of law cited below is reproduced in the regulatory Appendix attached to this Model.

RISK AREAS

The risk is obviously abstract and occurs only when criminal proceedings are brought (even if only in first instance proceedings), involving one or more senior officres or employees of the Company, and in which the parties in question have an interest, direct or indirect.

RECIPIENTS OF THE SPECIAL SECTION

The recipients of this special section are suspects and the accused in criminal proceedings for crimes committed during their normal duties within the Company, as well as all those who, by virtue of their hierarchical position or for other reasons, may have a real interest in the content of testimony given in legal proceedings.

CODE OF CONDUCT

It is expressly prohibited for all recipients of the Model:

- to incite anyone, including through a third party, using violence or threats or offers or promises of money or other benefits, not to testify or to bear false witness to promote the interests of the Company or to ensure that it gains an advantage;
- to influence, in any way, a person that may be called upon to testify before the judicial authorities as regards his/her choice of whether or not to exercise the right to silence or with reference to the content of his/her statements.

All recipients must also comply with the following principles:

- all recipients are required to make honest statements that reflect the reality of the facts in relations with the judicial authorities;
- Anyone asked to testify before the judicial authorities in relation to work activity carried out must freely express their representation of the facts or exercise the right to silence, as granted by law; they must also maintain the strictest confidentiality in relation to the declarations issued and their subject, if the same are covered by investigative secrecy.

DUTIES OF THE SB

In relation to this type of crime, the duties of the SB are as follows:

- to examine any invitation to appear before the judicial authorities to testify (both during preliminary investigations and during the proceedings) received by senior officers or employees in relation to crimes committed during their normal duties within the Company; to this end, the SB must be promptly notified by the recipients of this special section of any summons to appear before judicial authorities to testify;
- to receive and examine any report from workers or any other person in the Company;
- if considered appropriate, to examine the proceedings papers relating to the trial in which the interested party is required to testify.

CHAPTER 11

CRIMES IN RELATION TO ILLEGAL IMMIGRATION

With Italian Legislative Decree no. 109 of 16 July 2012, Italy adopted the European provisions on sanctions against employers who employ non-EU citizens staying illegally in the country.

Among the rules of the cited regulatory text, Art. 2 extends criminal liability in accordance with Italian Legislative Decree 231/2001 also to companies that recruit foreign citizens not having a residence permit, if some particular conditions are in place (which will be discussed below).

The use of undeclared labour constitutes an example of 'economic' crime, where the liability of entities naturally lies; indeed, it is precisely through the employment of illegal immigrants that companies seek to generate significant profits, which also causes serious distortions to the economic system as a whole.

The incriminating rule of reference (Art. 22, paragraph 12-bis of Italian Legislative Decree no. 286/98, known as Consolidated Law on Immigration) punishes the employer who employs non-EU workers not having a residence permit, or whose permit has expired (the renewal of which has not been requested), or also those with a revoked or cancelled permit.

In order for the Company to be liable, it is necessary not only for the illegal recruitment to have been carried out in the interests or to the benefit of the entity, in accordance with the general principles, but it is also essential for one of the following conditions to have been met:

- more than three workers are employed;
- the workers employed are minors, below working age;
- the employed workers are subject to other, particularly exploitative working conditions pursuant to Art. 603-bis, paragraph 3 of the Italian Criminal Code (for example, that workers are exposed to situations of serious danger, with regard to the characteristics of the services to be provided and the working conditions).

With Italian Law no. 161 of 17.10.2017, additional criminal offences in relation to illegal immigration were included in Art. 25-duodecies of Italian Legislative Decree 231/01.

This is, in particular, the crime envisaged by Art. 12, paragraph 3, of Italian Legislative Decree no. 191/286 (Consolidated Law on Immigration) which punishes anyone who promotes, directs, organises, finances or transports foreigners into the country or conducts other actions aimed at illegally arranging their entry into the country if:

- the crime concerns the illegal entry or stay in the country of five or more persons;
- the life or safety of the person transported was endangered to enable his/her illegal entry or stay;
- the person transported was subjected to inhumane or humiliating treatment to enable his/her illegal entry or stay;
- the crime was committed by three or more people working together or using international transport services or counterfeit, altered or otherwise illegally obtained documents;
- the perpetrators have weapons or explosive materials available.

A crime pursuant to Italian Legislative Decree 231/01 is also constituted by that indicated in Art. 12, paragraph 5 of Italian Legislative Decree 286/98 which punishes anyone who, in order to obtain unjust

profit from the condition of illegality of the foreigner, facilitates their stay in the country in violation of the relevant regulations.

The articles of law cited above are reproduced in the regulatory Appendix attached to this Model.

RISK AREAS

The risk of committing the crimes in relation to illegal immigration in the Company activity is rather contained, due to the very small number of non-EU employees usually employed.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at the employer, as well as all persons who operate in the sector of human resources and personnel selection.

CODE OF CONDUCT

The recruitment of non-EU citizens by the Company is based upon the following general principles:

- it is prohibited to establish permanent, temporary or seasonal subordinate employment relationships with non-EU citizens staying illegally in the country;
- in particular, it is prohibited to employ foreign workers not having a residence permit or whose permit has been revoked or expired, and the renewal of which has not been requested;
- the employer is required to guarantee to the foreign worker the remuneration and insurance treatment envisaged by the laws in force and the applicable national collective labour agreements;
- in no case may non-EU citizens under the legal working age be employed;
- all documentation, both in electronic and paper format, relating to the employment relationship with non-EU employees must be stored in the Company archives and must be easily accessible.

DUTIES OF THE SB

In relation to the duties of the employer and the other persons required to comply with and apply the rules on immigration, the duties of the SB will be the following:

- to oversee the correct fulfilment of the duties of persons found in a position of guarantee with respect to the legitimacy of recruitments of employees (also non-EU);
- to receive and examine any report from workers or any other person in the Company;
- to carry out control activities, also randomly, in relation to the documentation contained in the personal file of the individual non-EU employee stored in the Company archives.

CHAPTER 12

ORGANISED CRIMES, DOMESTIC AND TRANSNATIONAL

Italian Law no. 146 of 16.03.2006 – "*Ratification and execution of the United Nations Convention and Protocols against transnational organised crime, adopted by the General Assembly on 15 November 2000 and 31 May 2007*" – extended the liability of entities to certain crimes if they have a 'transnational' dimension (Art. 10).

Art. 3 of that regulatory text defines what should be understood exactly by "transnational crime". In particular, a transnational crime is considered to be "the crime punished with the maximum term of imprisonment of at least four years, if an organised criminal group is involved, as well as:

- it is committed in more than one country;
- or it is committed in one country but a substantial part of its preparation, planning, management or control occurs in another country;
- or it is committed in one country but an organised military group engaged in criminal activities in more than one country is implicated in it;
  or it is committed in one country but has substantial effects in another country".

For the purposes of the Company activity, the crimes - including those taken into consideration by the indicated regulation - that may theoretically be of significance are the following:

- obstruction of justice (Art. 377 of the Italian Criminal Code)
- incitement not to testify or to bear false witness (Art. 377 bis of the Italian Criminal Code);
- personal aiding and abetting (Art. 378 of the Italian Criminal Code);
- conspiracy (Art 416 of the Italian Criminal Code);
- mafia-like conspiracy, domestic or foreign (Art. 416 bis of the Italian Criminal Code).

It should be noted that conspiratorial crimes (Art. 416 and Art. 416-bis of the Italian Criminal Code) are significant, in accordance with Art. 24 ter of the Decree, even if committed only within the country.

The articles of law cited above are reproduced in the regulatory Appendix attached to this Model.

RISK AREAS

The conspiratorial crimes identified above presuppose the establishment of relationships of any nature, directly or indirectly - or even at transnational level – with entities external to the Company forming part of conspiracies.

As, in particular, the offence of conspiracy (Art. 416 of the Italian Criminal Code) may be preordained to the commission of any crime, the risk areas are widespread and not localised within the field of specific company functions. This is also in light of the type of activity performed by IDN which involves continuous contact with external entities (customers, suppliers, etc.).

The following risk areas can therefore be identified:

- negotiation and stipulation of commercial contracts, both with private and public entities;
- purchase of goods and services;
- selection, management and assessment of suppliers;
- management of gifts, hospitality and entertaining expenses;
- management of donations and sponsorships;

- management of intercompany relationships;
- search and recruitment of personnel.

The list is obviously subject to changes and additions; if this becomes necessary, additional risk areas will be identified, with consequent preparation of specific rules of conduct and respective procedures.

In such cases, the SB is responsible for proposing to the Board of Directors any appropriate intervention on the text of the previous Special Section. The Board of Directors itself may also take similar initiatives autonomously.

RECIPIENTS OF THE SPECIAL SECTION

This Special Section is aimed at all persons who, as part of their role in the Company, are likely to come into contact with persons extraneous to IDN.

CODE OF CONDUCT

This Special Section, in addition to the specific principles of conduct relating to the individual risk areas, cites the general principles of conduct contained in the Code of Ethics.

All those who operate on behalf of the Company are required to act in conformity with principles of integrity, prudence, fairness and transparency.

In particular, it is prohibited for all Recipients to establish relationships with persons, entities, companies or associations in any form they are established, in Italy and abroad, known to or reasonably believed or suspected to form part of or in any case be linked to or hold relationships of any nature with conspiracies or groups, or in any case whose identity and correctness has not be carefully and diligently ascertained in a traceable and documented manner.

With reference to the areas most exposed to the risk of committing conspiratorial crimes, the Company is inspired by the following principles of control:

- monitoring of the execution of contracts;
- formal identification of roles, duties and responsibilities of persons who select suppliers;
- precise definition of the parameters that regulate the approval of suppliers and products.

DUTIES OF THE SB

It is the duty of the SB:

- to constantly check the completeness and effectiveness of the provisions of this Special Section;
- to check compliance with the rules of conduct contained in this Special Section, by the respective recipients;
- to carry out any assessment considered appropriate on the individual risk operations;
- to verify the correct archiving of documentation relating to relationships with public, state or European institutions;
- to analyse any report received in relation to possible violations of this Special Section or relating to the commission of illegal acts or even just "suspicious" acts, preparing a specific report to be sent to the Board of Directors and proposing, if necessary, the adoption of appropriate disciplinary measures.

CHAPTER 13

CRIMES IN RELATION TO INFRINGEMENT OF COPYRIGHT

The predicate offences indicated in Art. 25-novies of the Decree relating to the infringement of copyright (indicated in Italian Law 633/1941), are the following:

- disclosure of intellectual property via the electronic network (Art. 171);
- crimes in relation to software and databases (Art. 171-bis);
- crimes in relation to intellectual property used on radio, television and cinema networks or in literary, scientific or educational material (Art. 171-ter);
- violations in relation to the SIAE (Italian copyright collecting agency) (Art. 171-septies);
- tampering with devices for decoding audio-visual signals with conditional access (Art. 171-octies)

RISK AREAS

In this context, it is believed that the risk areas are focused in the IT structure and mostly relate to the possible use of non-original and/or unlicensed software.

More specifically:

- management of activities connected to the purchase and use of software, databases or any other product protected by copyright;
- use of resources and information of IT or electronic nature or any intellectual property protected by copyright.

The list is obviously subject to changes and additions; if this becomes necessary, additional risk areas will be identified, with consequent preparation of specific rules of conduct and respective procedures.

In such cases, the SB is responsible for proposing to the Board of Directors any appropriate intervention on the text of the previous Special Section. The Board of Directors itself may also take similar initiatives autonomously.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at all persons who are in possession of IT equipment attributable to IDN.

CODE OF CONDUCT

The "*IT devices and systems regulation*" regulates the use of IT devices and systems (telephones, email, shared folders, internet, etc.) by all personnel of the Italian companies of the De Nora Group and external collaborators to whom, for any reason, a company device has been provided. In particular, according to existing company rules:

- access to data resources in electronic format occurs only via computers protected by username and password;
- for each computer and communication system, the user ID must identify only one user. for each system access, authorisation levels are established as necessary;
- passwords must always be encrypted and must not be stored in legible format in places where unauthorised people may discover and/or use them;
- devices and programmes must only be installed and updated by personnel instructed to do so;
- the servers are protected by corporate antivirus systems;

- any change of working status of employees within the Company (consultants, temporary or contracted) must be communicated immediately by the human resources department to the information system administrators involved;
- the Company exercises access control to the systems in protection of the integrity of the data which are kept on the computers and communication systems. The security manager and the network administrator may restrict or revoke any privilege for users; demand that the user deactivates or removes data, programs or other system resources that may threaten these objectives; consider any other solution necessary to manage and protect the IT system.

The Recipients are prohibited from:

- duplicating, importing, distributing, selling, granting on lease, disseminating, possessing, without being entitled to do so, computer programmes, protected databases or any work protected by copyright and by the related rights.

DUTIES OF THE SB

In relation to the duties of persons required to comply with the rules regulating copyright, the duties of the SB will be the following:

- to receive and examine any report from workers or any other person in the Company;
- to carry out control activity, also randomly, in relation to the existence and validity of the software licences on computer devices used by employees.

CHAPTER 14

CRIMES AGAINST THE INDIVIDUAL

Art. 25-quinquies of Italian Legislative Decree no. 231/01 governs certain crimes against the individual, likely to render the entity administratively liable if committed in its interests and/or to its benefit.

These crimes include, in particular, enslavement or keeping in slavery (Art. 600 of the Italian Criminal Code); child prostitution (Art. 600-bis of the Italian Criminal Code); child pornography (Art. 600-ter of the Italian Criminal Code); possession of pornographic material of minors aged under 18 (Art. 600-quater of the Italian Criminal Code); virtual pornography (Art. 600-quater1 of the Italian Criminal Code); tourism initiatives aimed at the exploitation of child prostitution (Art. 600-quinquies of the Italian Criminal Code); human trafficking (Art. 601 of the Italian Criminal Code); buying and selling of slaves (Art. 602 of the Italian Criminal Code).

Italian Law no. 199 of 29.10.2016 introduced, into the aforementioned Art. 25-quinquies, also Art. 603-bis of the Italian Criminal Code ("Illegal intermediation and exploitation of labour"), which punishes illegal recruitment through gangmasters ["caporalato" in Italian].

The latter expression refers to a typical distortion of the labour market. The gangmaster intermediates by recruiting labourers, often unspecialised, before placing them with employers, while claiming a percentage of their wages as remuneration.

The crime therefore punishes the conduct of anyone who:

- recruits labourers for use by third parties under exploitative conditions, by taking advantage of their hardship;
- uses, recruits or employs labour, including through the gangmastering referred to in the previous point, subjecting workers to exploitative conditions and taking advantage of their hardship.

In accordance with criminal law, an "indicator of exploitation" is the existence of one or more of the following conditions:

1) the repeated payment of wages in clear breach of national or regional collective bargaining agreements concluded by the most representative national trade union organisations, or wages clearly disproportionate to the quantity and quality of the work provided;
2) the repeated infringement of regulations on working hours, rest periods, weekly rest days, compulsory leave, holidays, etc.;
3) the existence of violations of workplace health and safety regulations; 4) subjecting workers to degrading working conditions, supervision methods or accommodation.

The articles of law cited above are reproduced in the regulatory Appendix attached to this Model.

RISK AREAS

The Group's Code of Ethics ("Code of Ethics", "Compliance and Safeguards" section) enshrines the principle whereby the Company promotes protection of the well-being of each individual employee so that everyone may work in an environment characterised by mutual respect and where no discrimination is tolerated.
The risk that crimes against the individual may be committed within the Company to facilitate any interest and/or advantage of the entity can be estimated as extremely low. Although it may be extremely limited,

the risk can be restricted to the crime of "gangmastering" not only in relation to the treatment reserved for internal staff but also with reference to the acquisition of goods from third parties who may be liable for the crime of illegal intermediation and exploitation of labour.

The risk areas can therefore be identified as follows:

- search, recruitment and management of personnel;
- purchase of goods and services;

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at the employer, as well as all persons who operate in the sector of human resources and the procurement of goods and services.

CODE OF CONDUCT

With reference to the search for, selection and recruitment of personnel:

- it is forbidden to establish open-ended, fixed-term or seasonal employment relationships through intermediaries who claim a percentage of the employee's remuneration;
- the employer is required to guarantee each worker the remuneration and insurance treatment envisaged by laws in force and the applicable national collective labour agreements;
- all documentation, both in electronic and paper format, relating to the employment relationship, must be stored in the Company archives and must be easily accessible.

With reference to the purchase of goods and/or services, the corporate functions must adhere to the following principles:

- to behave correctly, transparently and collaboratively, in compliance with the rules of law and internal company procedures, in all activities aimed at the administrative management of suppliers/customers/commercial partners, domestic or foreign;
- in particular, the commercial and professional reliability of suppliers and commercial/financial partners must always be verified based upon some significant indicators (e.g. public prejudicial data - protests, insolvency proceedings - or acquisition of commercial information on the company, the shareholders and the directors by way of specialist companies; price amount disproportionate to average market values);
- not to hold commercial relationships with persons (natural or legal) known to belong to criminal organisations or in any case operating outside of the law.

DUTIES OF THE SB

In relation to the duties of the employer and the other persons required to comply with and apply the rules on immigration, the duties of the SB will be the following:

- to oversee the correct fulfilment of the duties of persons found in a position of guarantee with respect to the legitimacy of recruitments of employees (also non-EU);
- to receive and examine any report from workers or any other person in the Company;
- to carry out control activities, also randomly, in relation to the documentation contained in the personal file of the individual non-EU employee stored in the Company archives.

CHAPTER 15

CRIMES IN RELATION TO RACISM AND XENOPHOBIA

Italian Law no. 167 of 20.11.2017 introduced Art. 25-terdecies into Italian Legislative Decree 231/01. This article extends the liability of a legal entity also to the crimes referred to in Art. 3, paragraph 3-bis, of Italian Law no. 654 of 13.10.1975 ("Ratification and implementation of the international convention on the elimination of all forms of racial discrimination").

This crime punishes any organisation, association, movement or group whose aims include propaganda or incitement to discrimination and violence for racial, ethnic, national or religious reasons. In particular, punishment is subject to the fact that such conduct, committed in a way that poses an actual risk of spread, is founded wholly or in part on the denial, serious minimisation or condoning of the holocaust or crimes of genocide, crimes against humanity and war crimes.

Therefore, the only relevant crime here is the most serious form of offences concerning incitement to racial hatred or the denial and/or minimisation of genocide, crimes against humanity and war crimes.

The article of law cited above is reproduced in the regulatory Appendix attached to this Model.

RISK AREAS

Within the Company, the crime risk appears genuinely residual and limited, if at all, to a potential improper use of the IT resources assigned to each employee, used for propaganda, in concert with others, aimed at racial hatred.

This indication is obviously subject to changes and additions; if this becomes necessary, additional risk areas will be identified, with consequent preparation of specific rules of conduct and respective procedures.

In such cases, the SB is responsible for proposing to the Board of Directors any appropriate intervention on the text of the previous Special Section. The Board of Directors itself may also take similar initiatives autonomously.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at all persons who are in possession of IT equipment attributable to IDN.

CODE OF CONDUCT

The "*IT devices and systems regulation*" regulates the use of IT devices and systems (telephones, email, shared folders, internet, etc.) by all personnel of the Italian companies of the De Nora Group and external collaborators to whom, for any reason, a company device has been provided. In particular, according to existing company rules:

- access to data resources in electronic format occurs only via computers protected by username and password;
- for each computer and communication system, the user ID must identify only one user. for each system access, authorisation levels are established as necessary;
- passwords must always be encrypted and must not be stored in legible format in places where unauthorised people may discover and/or use them;

- devices and programmes must only be installed and updated by personnel instructed to do so;
- the servers are protected by corporate antivirus systems;
- any change of working status of employees within the Company (consultants, temporary or contracted) must be communicated immediately by the human resources department to the information system administrators involved;
- the Company exercises access control to the systems in protection of the integrity of the data which are kept on the computers and communication systems. The security manager and the network administrator may restrict or revoke any privilege for users; demand that the user deactivates or removes data, programmes or other system resources that may threaten these objectives; consider any other solution necessary to manage and protect the IT system;
- the network units are areas for sharing purely professional information and they may not be used, in any way, for other purposes;

The Recipients are prohibited from:

- propagating ideas based on racial or ethnic superiority or hatred, or committing or inciting others to commit acts of discrimination for racial, ethnic, national or religious reasons;
- committing or inciting others to commit violence or acts inciting violence for racial, ethnic, national or religious reasons;
- participating in organisations, associations, movements or groups whose aims include incitement to discrimination or violence for racial, ethnic, national or religious reasons.

DUTIES OF THE SB

In relation to the duties of persons required to comply with the rules regulating copyright, the duties of the SB will be the following:

- to receive and examine any report from workers or any other person in the Company;
- to carry out control activity, also randomly, in relation to the existence and validity of the software licences on computer devices used by employees.

CHAPTER 16

TAX CRIMES

Art. 25-quinquiesdecies of Italian Legislative Decree 231/01 regulates the liability of the Company for some criminal offences in relation to taxes introduced by Italian Law no. 157/2019 converting Decree Law no. 124/2019.

The crimes considered by Italian Legislative Decree 231/01 and that could be committed as part of the activity carried out by IDN are the following:

Fraudulent misrepresentation using invoices or other documents for non-existent transactions (Art. 2 of Italian Legislative Decree 74/2000)
This type of crime punishes those who indicate in one of the mandatory annual returns (income tax or VAT) fictitious payable elements in order to evade the tax and, for that purpose, use invoices or other documents, referring to non-existent transactions and that constitute evidence of these transactions.

Fraudulent misrepresentation by means of other deception (Art. 3 of Italian Legislative Decree 74/2000)
This type of crime punishes those who, by completing objectively or subjectively simulated transactions or by using false documents or other fraudulent means likely to hinder the assessment and to mislead the Tax Administration, indicate in one of the returns for those elements of taxes payable for an amount less than the actual sum or fictitious payable elements or fictitious receivables and withholdings in order to evade income tax or value added tax.

Issuance of invoices or other documents for non-existent transactions (Art. 8 of Italian Legislative Decree 74/2000)
This type of crime punishes those who issue or transmit invoices or other documents for non-existent transactions in order to allow third parties to evade income tax or value added tax.

Concealment or destruction of accounting documents (Art. 10 of Italian Legislative Decree 74/2000)
This type of crime punishes those who conceal or destroy, in whole or in part, accounting records or documents which must mandatorily be retained, so as to prevent the reconstruction of the income or turnover, in order to evade income tax or value added tax, or to allow third parties to evade them.

Fraudulent evasion of tax payments (Art. 11 of Italian Legislative Decree 74/2000)
This type of crime punishes those who:

- alienate by simulation or complete fraudulent acts on their own assets or those of others to render ineffective - in whole or in part - the procedure of compulsory collection in order to evade the payment of income tax or value added tax or interest or administrative sanctions relating to those taxes;
- indicate, in the documentation submitted for the purposes of the tax settlement procedure, receivable elements for an amount less than the actual amount or fictitious payable elements for an amount overall greater than fifty thousand Euros in order to obtain for themselves or for others a partial payment of taxes and related accessory costs.

False statement in a tax return (Art. 4 of Italian Legislative Decree 74/2000)
This type of crime punishes those who indicate receivable elements less than the actual amounts or non-existent payable elements in the annual VAT and/or income tax returns when, jointly:

- the tax evaded is higher, with reference to any of the individual taxes, than one hundred thousand Euros;
- the total amount of receivable elements removed from taxation, also by indicating non-existent payable elements, is greater than ten per cent of the total amount of receivable elements indicated in the return, or, in any case, more than two million Euros.

This is a crime punishable in accordance with Italian Legislative Decree 231/01 only in the circumstance where it:

- presents the nature of transnationality (an organised criminal group is involved, as well as: a) it is committed in more than one country; b) or it is committed in one country but a substantial part of its preparation, planning, management or control occurs in another country; c) or it is committed in one country but an organised criminal group engaged in criminal activities in more than one country is implicated in it; d) or it is committed in one country but has substantial effects in another country);
- it was committed for the purpose of evading VAT for an amount no less than ten million Euros.

Failure to file a tax return (Art. 5 of Italian Legislative Decree 74/2000)
This type of crime punishes those who:

- do not file VAT or IRPEF returns in order to evade the respective taxes;
- do not file the withholding agent return (if obliged to do so) provided that this concerns withholdings not paid for an amount greater than fifty thousand Euros.

This is a crime punishable in accordance with Italian Legislative Decree 231/01 only in the circumstance where it:

- presents the nature of transnationality (an organised criminal group is involved, as well as: a) is committed in more than one country; b) or is committed in one country but a substantial part of its preparation, planning, management or control occurs in another country; c) or is committed in one country but an organised criminal group engaged in criminal activities in more than one country is implicated in it; d) or is committed in one country but has substantial effects in another country).
- it was committed for the purpose of evading VAT for an amount no less than ten million Euros.

Illegal offsetting in a tax return (Art. 10-quater of Italian Legislative Decree 74/2000)
This type of crime punishes those who:

- do not pay the sums due by offsetting their payables against receivables not due for an annual amount greater than fifty thousand Euros;
- do not pay the sums due by offsetting their payables against non-existent receivables for an annual amount greater than fifty thousand Euros.

This is a crime punishable in accordance with Italian Legislative Decree 231/01 only in the circumstance where it:

- presents the nature of transnationality (an organised criminal group is involved, as well as: a) is committed in more than one country; b) or is committed in one country but a substantial part

of its preparation, planning, management or control occurs in another country; c) or is committed in one country but an organised criminal group engaged in criminal activities in more than one country is implicated in it; d) or is committed in one country but has substantial effects in another country).

- commit the crime for the purpose of evading VAT for an amount no less than ten million Euros.

RISK AREAS

In light of the crimes and conduct cited above, the Company's areas of activity considered most at risk of commission of illegal activities can be identified as follows:

A. Management of tax obligations and, in particular:

- Management of accounting and taxes (tax returns and any controls on the correct keeping of records and on tax amounts);
- Preparation, signature and submission of tax returns
- Management of relationships with the Tax Authority
- Management of relationships with external tax advisors.

B. Purchasing cycle and, in particular:

- Purchase requests for goods and/or services
- Database management/register of suppliers/consultants
- Selection of suppliers/consultants
- Payments

C. Sales and distribution cycle and, in particular:

- Issuance and recording of invoices receivable
- Receipts

D. Management of intercompany relationships and, in particular:

- Intercompany transactions
- Intercompany services and respective allocation of costs
- Transactions of an ordinary and extraordinary nature

The list is obviously subject to changes and additions; if this becomes necessary, additional risk areas will be identified, with consequent preparation of specific rules of conduct and respective procedures.

In such cases, the SB is responsible for proposing to the Board of Directors any appropriate intervention on the text of the previous Special Section. The Board of Directors itself may also take similar initiatives autonomously.

RECIPIENTS OF THE SPECIAL SECTION

This special section is aimed at the Directors and all employees who take part in one of the processes relating to the risk activities highlighted above with particular - but not exclusive - reference to the AFC,

Procurement and Legal departments, as well as to the Board of Statutory Auditors, the Independent Auditor and the external tax advisors.

CODE OF CONDUCT

The Company undertakes to completely and transparently fulfil all tax obligations envisaged for it and to collaborate, where necessary, with the tax authority.

Tax returns and tax payments are mandatory fulfilments which cannot be evaded; all conduct aimed at avoiding tax obligations for the Company are therefore prohibited.

In particular, in addition to what is already envisaged in Chapters 3 (corporate crimes), 4 (crimes against Public Administration), 6 (cyber crimes), 8 (crimes of receiving, laundering, reusing and self-laundering) and 10 (organised crimes, domestic or transnational), it is mandatory to comply with the following.

Management of tax obligations

Tax obligations must be fulfilled by the legal deadlines, subject to appropriate planning and in compliance with principles of truthfulness, transparency and completeness.

In general, it is prohibited:

- to indicate non-existent liabilities or assets in an amount lower than the actual value, also using invoices for non-existent transactions or other deception;
- to issue invoices for non-existent transactions;
- to fraudulently evade the payment of taxes;
- to conceal or destroy tax documents;
- to indicate in the annual returns (VAT and IRES corporate income tax) receivable elements for an amount less than the actual amount or non-existent payable elements;
- to use receivables not due or non-existent to offset tax, social security and/or welfare payables.

In particular, the Company must:

- constantly monitor, also through a schedule, its tax compliance;
- complete the mandatory tax returns (e.g. annual income declaration, VAT, etc.) in the terms and methods envisaged by law (e.g. correctly identifying the signatory, submitting the returns on the correct forms, having the returns signed by the Legal Representative or by his/her delegate) and in compliance with principles of truthfulness, transparency and completeness;
- to verify the correctness of the data indicated in the tax returns (e.g. existence of receivables used for offsetting);
- to have the tax returns signed by the person delegated for that purpose (where present) or by the Legal Representative;
- to submit the tax returns by legal deadlines:
- to store in a specific archive (also electronic) all accounting and support documentation and make it available to the competent authorities (e.g. deposit receipts/submission of VAT returns);
- to handle any relationships and contacts with persons belonging to the Tax Authority in compliance with Chapter 4 (crimes against Public Administration) of this Model as well as with the Code of Ethics.

In the event of inspections/accesses/requests by the Tax Authority, it is mandatory to monitor and keep a track of all tax audit activities implemented in relation to the Company as well as the individual accounts held by the individual company departments;
- to handle relationships with external tax advisors in compliance with this Model and the Code of Ethics.

Sales and distribution cycle and purchasing cycle

The Company is required to manage the sales and distribution cycle and the purchasing cycle in compliance with existing regulations, the principles of the Code of Ethics, Chapter 7 (crimes of receiving, laundering and use of money, assets or gains of illegal origin), as well as in compliance with the procedures and provisions adopted by IDN, which are binding for all Group Companies.

In general, the issuance and/or use of any tax document must be preceded by:
- referencing of the supplier/consultant, by verifying the effectiveness and existence of the respective activity;
- pertinence check of the service provided by the supplier/consultant to the business activity;
- conformity check of the service with respect to that stated in the purchase request and contractually agreed, or correspondence check between the order/contract signed with the customer and the service provided;
- validation of documentation regarding the correspondence and truthfulness of the documentation with respect to the supply/service;
- check that the service has been provided between the entities indicated in the invoice.

In the event of anomalies which infer (alternatively) that
- the supplier/consultant is an entity that is essentially inoperative, or fiscally in default,
- the service (incoming and outgoing) has not been effectively provided in whole or in part,
- the service was provided between entities different from those indicated in the respective tax document,

it is compulsory to duly inform the SB.

It is mandatory to retain all documentation relating to the sales and distribution cycle and the purchasing cycle in a specific archive (also electronic) and to make it available to the Authorities.

Management of receipts and payments

In relation to the management of receipts and payments, the company has:
- adopted a system to check the legality of financial transactions or donations/receipts of any other benefit, with reference to the consistency between the contract, the service/goods provided/received, the invoice and the payment/receipt and that contractually agreed;
- adopted suitable measures to protect the IT systems used in the process in question, as well as specific authorising protocols;
- defined specific rules for managing exceptions to the procedures to be applied in cases expressly envisaged (e.g. urgent payments, payments without a purchase order and/or not managed by the system);
- introduce a delegations system with respect to restrictions, spending limits and responsibilities with regard to payment instructions;
- identified roles and responsibilities for authorising, executing and checking payments;

- defined duties and responsibilities of the areas/parties that request, authorise and execute payments.

In particular, in relation to receipt and payment activities, in compliance with the general principles adopted by the company, it is not permitted:

- to make payments or recognise reimbursements of expenses, compensation, discounts, advances or credit notes or any other form of reduction of the sum owed to internal or third parties which:
  - are not adequately justified in the light of the contractual relationship established with said parties;
  - are not made in return for goods, services, etc. actually received by the Company;
  - are not motivated by objective factors and justified by suitable documentation;
  - are not owed by the Company because of legal obligations.
- to use money or other bearer instrument for any collection or payment transaction, transfer of funds, any use of financial assets, or utilise anonymous current or savings accounts or those bearing a false name; exceptions to the use of money or other bearer instrument may be permitted for modest amounts and will be governed by specific internal regulations;
- to make payment to a party other than the contractual counterparty;
- to make payments that do not exactly correspond to those indicated in the contract/purchase order;
- to make payments to current accounts of banks belonging to or operating in countries listed as tax havens, or to offshore companies. Any exceptions to this prohibition must be authorised by an adequate hierarchical level and communicated to the SB;
- to accept and execute payment orders from unidentifiable parties, not listed in the register and whose payments cannot be traced (amount, name/title, address and current account number) or where, after the checks made when opening/modifying the register of suppliers/customers on the system, full correspondence cannot be guaranteed between the name of the supplier/customer and the holder of the account into/from which the payment will be made.

Management of intercompany transactions

Intercompany financing transactions must occur in compliance with any specific Group procedures, which must describe the operating flow and the management process of intercompany loans, both loans of ordinary and extraordinary nature.

Any commercial and/or financial transactions at Group level must occur according to market values, identified in accordance with specific criteria and by the specific company departments, in compliance with industry regulations.

In managing cash flows, it is mandatory to carry out the periodic reconciliation of any intercompany transactions.

DUTIES OF THE SB

It is the duty of the SB:

- to check compliance with the rules of conduct contained in this Special Section, by the respective recipients;
- to carry out control activities, also randomly, on individual risk operations;

- to check any assessment and dispute reports for the Company;
- to analyse any report received in relation to possible violations of this Special Section or relating to the commission of illegal acts or also simply "suspicious" acts.

In addition, the SB may:

- request a meeting with the independent auditing company;
- request a meeting with the external tax advisor;
- request information on the management of any beneficial tax regimes;
- request information on any discussions with the Tax Authority.

CHAPTER 17

CRIMES OF MARKET ABUSE

This chapter refers to the crimes of market abuse; the aim of this chapter is to identify the procedures as well as the rules that all managers, employees and collaborators of the Company must follow in order to prevent the occurrence of episodes of market manipulation.

Art. 185 of Italian Legislative Decree no. 58 of 24.02.1998 (Consolidated Finance Law) punishes with imprisonment from one to six years and with a fine from twenty thousand Euros to five million Euros "*anyone who spreads false information or implements simulated transactions or other trickery likely to cause a significant alteration in the price of financial instruments*".

The crime therefore materialises in the conduct of anyone who spreads false information or implements simulated transactions, likely to cause a significant alteration in the price of financial instruments.

While, on the one hand, it is true that IDN is an unlisted company and is therefore not present on the financial markets, on the other, the fact must be considered that the Group's shareholders may include listed companies which, by reflection, could therefore theoretically suffer repercussions on the price of the respective stock if false information is spread or simulated transactions are implemented.

It is therefore also appropriate to assess and include this type of crime in this model, consequently adopting the necessary protocols to protect the company and its employees.

RISK AREAS IDENTIFIED

The main risk areas identified are the following:

- Administration, Finance and Control (AFC);
- Sales & After Sales;
- Global Operations;
- HR, Organisation & Int. Communication.
- Marketing, Business Development and Product Management.

CODE OF CONDUCT, PROCEDURES APPLIED AND CONTROL MEASURES

The Company undertakes to respect scrupulously all laws in force and, in particular, in completing transactions of any nature on financial instruments or in spreading information relating to the same, it ensures compliance with the principles of correctness, transparency, completeness of information, protection of the market and compliance with the dynamics of free determination of the stock price.

From that perspective, it is strictly prohibited to spread, in any way, false information, news or data or to implement fraudulent or misleading transactions even if only potentially likely to cause an alteration in the price of financial instruments.

In particular, the Company undertakes:

a) always to behave with diligence, fairness and transparency, in the interest of the public, investors and the market;
b) to organise itself in such a way as to exclude the occurrence of situations of conflict of interest and, on those occasions, to guarantee balanced protection of the conflicting interests;

c) to adopt measures to ensure that there is no undue circulation/dissemination, within the Company and the Group, of significant information.

With regard to the management of privileged information, such as, by way of example, information on new products and markets, accounting data of the period, quantitative targets relating to the operating performance, capital transactions, it is strictly prohibited to disseminate that information outside the Company.

To that end, the company regulation envisages:

- the obligation to keep private the information acquired in carrying out company duties and to use private documents and information exclusively for performance of the role;
- the storage and archiving of all confidential documentation, acquired in carrying out the duties, in a location which only allows access to authorised persons;
- the establishment of specific contractual precautions, aimed at regulating the processing of and access to privileged and confidential information by consultants/commercial partners through the establishment of specific confidentiality clauses and clauses requiring compliance with the Code of Ethics and the Model adopted by the Company.

In the case of transmission, certain authorisation processes are in place to ensure that such information is made official in nature.

At meetings of the Board of Directors, the information produced is brought to the attention of the competent functions by subject and sent to a single company office that channels the respective information flows. All documentation is archived and kept confidential by the competent offices.

As part of the management of relationships with the media and the dissemination of new and/or advertisement of goods/services (general press, specialist press, update of internet website), in line with the principles of conduct and control established by the Parent Company, the regulation envisages:

- the formal identification of the company officers instructed to establish the communication strategies and to deal with external relationships and media relations;
- the formal approval of press releases prior to their respective public disclosure, as well as the archiving of documentation relating to publications with the respective decision-making flows.

Management of external communications

With regard to the management of external information flows, a function is identified, in the regulation of the Parent Company, to establish the commercial communication strategies and to deal with external relationships and media relations.

The same structure establishes the *format* and the guidelines of the internet website and also deals with information flows between the functions involved in obligations relating to the constant update of the institutional website. The documentation relating to requests for publications, received from the competent Organisational Units, the publications made and the decision-making flows are archived by the function in charge.

To complete the above, it should be noted that the IT security of the data is guaranteed by protocols controlling "*Cyber crimes*" (see chap. 6).

As part of the sensitive activity of managing privileged information relating to the Company such as, by way of example, information on new products and markets, accounting data for the period, quantitative

targets relating to the operating performance, capital operations, the managers have been identified who, potentially, due to the role covered or the functions performed, may hold or produce privileged information.

DUTIES OF THE SB

The Supervisory Body has the power to perform specific checks, also as a result of reports received; the Body also has the right to access all company documentation available in the matter, with no obligation to provide prior notice.

The Company has also established information flows suitable to allow the SB to acquire useful information for monitoring communications and relevant transactions in relation to market abuse.

In particular, the procedure relating to the external disclosure of information concerning extraordinary transactions establishes that those responsible for commercial communication strategies and external relations must request and obtain express authorisation from the CEO.

The Supervisory Body, in carrying out the activities indicated above, may make use of all competent resources in this regard.