ORGANISATION, MANAGEMENT AND CONTROL MODEL

DIERRE S.P.A.

pursuant to Italian Legislative Decree no. 231 of 8 June 2001 as further amended and supplemented

approved for the first time by the Board of Directors on 2 March 2017

Update: January 2025

TABLE OF CONTENTS

General Section

Special Section

Special section	Description
A	Code of ethics
B	Organisational structure and system of delegations
C	Structure, composition, regulations and functioning of the Supervisory Body
D	Sanctions system
E	Offences against the Public Administration and against the State
F	Offences relating to the counterfeiting of legal tender, public credit instruments, revenue stamps and identification tools or signs
G	Corporate offences
H	Offences against the individual
I	Offences relating to workplace safety
J	Offences relating to the receipt, laundering or use of money, goods or benefits of unlawful origin, as well as self-laundering
K	Offences relating to cybercrime and unlawful data processing
L	Offences relating to copyright infringement
M	Crimes against industry and commerce
N	Offences pursuant to Article 377-bis of the Italian Criminal Code
O	Offences relating to organised crime
P	Environmental crimes
Q	Offences related to the employment of illegal immigrants
R	Transnational offences referred to in Italian Law no. 146 of 16 March 2006
S	Tax offences
T	Offences relating to smuggling
U	Offences relating to non-cash means of payment
Compliance manual –	
Reporting procedure -	Whistleblowing

1. LEGISLATIVE DECREE NO. 231 OF 8 JUNE 2001

Italian Legislative Decree No. 231 of 8 June 2001 (hereafter 'the Decree'), which came into force on 4 July 2001, sets out the 'Regulations on the administrative liability of legal entities, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of 29 September 2000'. The Decree was intended to bring Italian legislation on the liability of legal entities into line with international conventions to which Italy had long been a signatory. In particular, it aligns Italian legislation with the following conventions:

- the Brussels Convention of 26 July 1995 on the protection of the European Community's financial interests,
- the Brussels Convention of 26 May 1997 on combating corruption involving officials of the European Communities or officials of Member States of the European Union,
- the OECD Convention of 17 December 1997 on Combating Bribery of Foreign Public Officials in International Business Transactions.

This Decree introduced a system of administrative liability for legal persons (or: "companies") into Italian law that is comparable to criminal liability (1). This liability is in addition to that of the individual who committed certain offences and aims to include companies in the punishment for these offences if they were committed for their benefit.

The liability set out in the Decree also applies to offences committed abroad, provided that the country in which the crime was committed does not initiate legal proceedings.

The entity shall be liable even if the offender has not been identified, and shall remain liable even if the offence itself is extinguished with respect to the offender for any reason other than amnesty or the statute of limitations. Administrative sanctions against the entity expire within 5 years of the date on which the offence was committed, unless the statute of limitations is interrupted.

1.1. Principle of legality

The entity's liability is limited by law. According to art. 2 of the Decree, the entity "cannot be held liable for an offence if its [criminal] liability and related sanctions are not expressly provided for by a law in force before the offence was committed".

1.2. Objective criteria for attributing liability The objective

criteria for attributing liability fall into three categories:

a) committing an offence specified in articles 24 to 25-*duodecies* of the Decree.
b) The offence must have been committed "in the interest or to the advantage of the entity".

Interest and/or advantage

Another element that constitutes the liability in question is that the alleged unlawful conduct must have been committed in the interest of, or to the advantage of, the Entity.

The entity's interest or advantage is considered the basis for its liability, even when the interests or advantages of the perpetrator or third parties also apply. The only exception to this is when an offence is committed by an individual in a senior position within the entity; in this case, the liability lies exclusively with the offender or third parties.

(1) The "criminal" nature of this liability can be deduced from the following four elements: 1) it derives from an offence, in that the offence is a prerequisite for the sanction; 2) it is ascertained by a criminal magistrate with the associated guarantees of the criminal process; 3) it involves the application of sanctions, such as pecuniary and restrictive ones; 4) guilt plays a central role, in line with the principle of culpability.

Since no exempting effect has been recognised for the exclusive “advantage” of the offender or third parties, but only - as stated - for the exclusive interest of these individuals, the entity should be held liable even if it does not obtain any advantage or if an exclusive advantage is obtained by the offender or third parties. This applies provided that the entity has an interest that may conflict with that of third parties in the offences committed by individuals in senior positions within its organisation.
Therefore, the liability provided for by the Decree arises not only when unlawful conduct results in an advantage for the entity itself, but also when an unlawful act is justified in the entity's interest, even in the absence of such a concrete result. In short, the two terms express distinct legal concepts and presuppositions, each with its own autonomy and scope of application.
Regarding the meaning of the terms “interest” and “advantage”, the government Report accompanying the Decree attributes a markedly subjective value to the former, susceptible to an *ex ante* evaluation (known as benefit-focused), and a markedly objective value to the latter. The latter refers to the actual results of the acting party's conduct. Even if the individual did not directly focus on the entity’s interest, they nevertheless achieved an advantage in its favour through their conduct, This advantage is susceptible to *ex post* verification.
The essential features of interest are identified as: objectivity, understood as being independent of the agent’s personal or psychological beliefs and rooted in verifiable external elements that can be observed by anyone; concreteness, understood as registering the interest in actual existing phenomena, to safeguard the principle of harm; actuality means that the interest must objectively exist and be recognisable at the time the act is recognised, and it must not be future or uncertain; otherwise, the required damage to the property for classification as an offence rather than mere danger is lacking. Economic relevance is not necessary, but it can also be attributable to a corporate policy.
In terms of content, the advantage attributable to the entity – which must be kept separate from profit – can be: direct, meaning it is attributable exclusively and directly to the entity, or indirect, meaning it is mediated by results acquired by third parties which are likely to have a positive impact on the entity. It can also be financial, even if not necessarily immediate.

“Group” interest

The Court of Cassation (Sec. V, 17 November 2010 - 18 January 2011, Public Prosecutor, Court of Bari, in the case of Tosinvest Servizi S.r.l. et al.) addressed the issue of the criteria for allocating administrative liability, as set out in Legislative Decree no. 231 of 2001, within a *holding* company or other companies that form part of a group to which one of the entities has been directly attributed with the liability in question, by virtue of criminal conduct carried out by individuals in positions of authority, as defined in art. 5 paragraph 1. This was the first time that this issue had been addressed.
Despite corporate groups being widespread in the modern economy, previous rulings on the matter had already partially established the guidelines for extending administrative liability to the various components of a group of companies. These rulings addressed an issue that is completely ignored by the current regulatory framework.

The first limitation to this expansive liability was identified in the subjective attribution criteria set out in the Decree, according to which there must be a relationship between the entity in question (whether a holding, parent company or subsidiary) and the perpetrator of the predicate offence. The perpetrator must hold a senior or subordinate role within the same entity as those exercising management or supervisory prerogatives (Court of Milan, 20 December 2004, in *www.rivista231.it*; Court of Milan, 14 December 2004, Cogefi, in *Foro It.*, 2005, II, 527).
Another factor that extends liability is the so-called “group interest”, which is sometimes given the same importance as that attributed to it in the Civil Code following the reform of corporate law,

and civil case law (Court of Milan, 20 September 2004, Ivri Holding et al, in *Foro It.*, 2005, 556) and on other occasions, starting from the attribution criteria outlined in the Decree, (particularly Articles 5(2), 12(1)(a) and 13(final paragraph)), read in the light of the substantial connections between the entities involved (Preliminary investigations judge, Court of Milan, 26 February 2007, Fondazione M. et al, in La responsabilità amministrativa delle società e degli enti *(The administrative liability of companies and entities*, 2007, 4, 139). From the perspective outlined above, given that the entity is not liable only if the person who committed the crime acted in their own exclusive interest or in the interest of a third party, it was deemed appropriate to exclude both the advantages obtained by the controlled company as a consequence of the parent company's activity and the activity of the latter being said to have been carried out in the exclusive interest of a third party. This is due to the inevitable repercussions that the conditions of the controlled company have on the parent company (Court of Milan, 20 December 2004, cit.). Ultimately, to establish the liability of a legal entity whose senior employee committed an offence for the benefit of, or to the advantage of, other entities within the same business group, it is necessary to identify links or connections between those entities. This prevents the favoured entity from being classified as a third party, as it appears that the offence was committed with the intention of benefiting several individuals, including those belonging to the perpetrator's legal entity. (EPIDENDIO, sub *Art. 5 Decree Law. 8 June 2001, no. 231*, cit., 9458).

In the case brought before the Supreme Court, the judge presiding over the preliminary hearing ruled that certain members of the group of companies led by the perpetrator had benefited from disputed practices. However, despite being part of the same financial group, no other companies derived any significant benefit, meaning no charges could be brought against them under the Decree.

In response to an appeal seeking to prove the opposite, and given that the individual in a senior position who was charged with corruption was in fact a de facto director of the companies deemed not to be involved, the Supreme Court specified the three conditions that must be met for an entity to be held liable. These are the commission of one of the predicate offences set out in the Decree; the commission of the offence by a person linked to the legal entity by organisational or functional relationships; and the pursuit of an interest or attainment of an advantage for the entity. These must be verified on a case-by-case basis.

With regard to the holding company and other group companies, other than the entity on whose behalf the perpetrator of the predicate offence acted, the second of the three conditions set out can be considered met when an individual acting on their behalf conspires with the person who committed the predicate offence. In this sense, generic references or membership of the same group as the entity directly affected by administrative liability are not decisive.

Regarding the additional predicate offence of interest or advantage, the holding or other group company can only be held liable under the Decree's provisions if they gain potential or real benefits, whether financial or otherwise, from the commission of the predicate offence, This must be verified on a case-by-case basis.

Ultimately, it seems that the Supreme Court endorses the argument that the interest of an entity (whether a parent company, controlling company or a subsidiary) in the commission of a predicate offence cannot be inferred from its belonging to a distinct group interest. Instead, it must be recognised and verified in concrete terms as being attributable to the legal person in question. This must be considered alongside the de facto or de jure connections with the various elements of the business group, particularly, the entity to which the principal perpetrator of the offending conduct belongs.

Interest and/or advantage in cases of negligence

Legislation on corporate criminal liability is generally based on alleged predicate offences of an intentional nature.

The introduction of negligent offences in the field of workplace safety – as set out in Law n. 123 of 3 August 2007, ("new" art. 25 *septies* later repealed and replaced by art. 300 Italian Legislative Decree 81 of 9 April 2008) – once more emphasised the importance of the issue of the subjective nature of the attribution criteria.
From this perspective, it is argued that in cases of negligence, the conceptual pair "interest / advantage" should not refer to unintended unlawful events, but rather to the conduct adopted by the individual when carrying out their activity. It is also stated that, from a structural point of view, negligent crime is difficult to reconcile with the concept of interest.
In this context, it can only be hypothesised that omitting behaviours required by precautionary regulations, intended to prevent workplace accidents, could result in reduced company costs that could be classified as an 'advantage' *ex post* as an "advantage" (for example, failing to provide protective equipment or failing to inspect equipment due to a need to save money).

c) The criminal offence must have been committed by one or more senior individuals, i.e. 'persons who hold representative, administrative, or managerial roles for the company or one of its organisational units with financial and operational autonomy', or persons who, even de facto, exercise the management and control" of the entity (i.e. holding 'senior roles'); or 'persons subject to the management or supervision of a senior individual' ('subordinates').
Individuals who commit an offence that may result in administrative liability for the entity may be: 1) individuals in "senior positions", such as the legal representative, director, CEO or facility manager, or individuals performing management and control functions within the entity, whether formally or de facto; 2) "subordinate" individuals, typically employees, but also individuals from outside the entity who have been entrusted with a task to be performed under the management and supervision of senior management personnel. If several individuals are involved in committing the offence (as in the case of conspiracy to commit a crime under *art.* 110 of the Italian Criminal Code), the "qualified" individual does not need to take the usual action provided for by criminal law. It is sufficient that they knowingly contribute to the commission of the crime.

1.3. Subjective criteria for attributing liability

The subjective criteria for attributing liability are met when the offence demonstrates a connotative approach in company policy, or when it depends on organisational negligence.
The provisions of the Decree exclude the entity's liability, if prior to the crime being committed, it had adopted and effectively implemented a suitable "organisational and management model" (referred to here as: "model") for preventing offences of type committed.
In this respect, liability is attributed to a "failure to adopt or comply with the required *standards*" relating to the entity's organisation and activities. This fault can be attributed to corporate policy or structural and prescriptive failings within the company's organisation.

1.4. Types of offences considered

The Decree covers the following offences:

- Offences against the Public Administration or against the State (Articles 24 and 25 of the Decree), as amended by Laws nos. 137/2023, 90/2024, 112/2024 and 114/2024:
    Misappropriation of public funds (art. 316 *bis* of the Italian Criminal Code);
    Undue receipt of public funds (art. 316 *ter* of the Italian Criminal Code);
    Fraud against the State or another public body or with the intention of exempting someone from military service (art. 640, paragraph 2, no. 1, of the Italian Criminal Code);

Aggravated fraud to obtain public disbursements (art. 640-*bis* of the Italian Criminal Code); Computer fraud (art. 640-*ter* of the Italian Criminal Code);
Bribery for the performance of an official act (art. 321 of the Italian Criminal Code);
Bribery to obtain an act in breach of official duties (art. 318 of the Italian Criminal Code);
Incitement to corruption (art. 322 of the Italian Criminal Code);
Extortion (art. 317 of the Italian Criminal Code.)
Bribery for an act contrary to official duties (articles 319, 319 *bis* and 321of the Italian Criminal Code);
Bribery in judicial proceedings (art. 319-*ter*, paragraph 2 and 321 of the Italian Criminal Code);
Undue incitement to give or promise benefits (art. 319 *quater*); Bribery of a public servant (art. 320 of the Italian Criminal Code);
Embezzlement, extortion, corruption and incitement to corruption of members of the bodies of the European Communities and of officials of the European Communities and of foreign states (art. 322-*bis* of the Italian Criminal Code);
Trading in influence (art. 346-*bis* of theItalian Criminal Code)
Fraud in public supplies (art. 356 of the Italian Criminal Code)
Fraud in the agricultural financing sector (art. 2 of Law n. 898 23 December 1986) Embezzlement (art. 314 of the Italian Criminal Code)
Embezzlement by taking advantage of another's error (art. 316 of the Italian Criminal Code)
Bid rigging (art. 353 of the Italian Criminal Code)
Interference with the tender process (art. 353 bis of the Italian Criminal Code)
Misappropriation of money or movable property (art. 314 bis of the Italian Criminal Code)

- by virtue of the promulgation and entry into force of Decree Law no. 350 of 25 September 2001, converted with amendments into Law no. 409 of 23 November 2001, and by virtue of the additions made to the promulgation and entry into force of Law no. 99 of 2009, *the offences set out in art. 25* bis *of the Decree, namely offences relating to the counterfeiting of legal tender, public credit instruments, revenue stamps and identification tools or signs*:

Counterfeiting of money, spending and introducing counterfeit money into the country, in conspiracy with others (article 453 of the Italian Criminal Code);
Alteration of currency (art. 454 of the Italian Criminal Code);
Spending and introducing counterfeit currency into the country, not in conspiracy with others (Article 455 of the Italian Criminal Code) Spending counterfeit money received in good faith (Article 457 of the Italian Criminal Code);
Counterfeiting of revenue stamps, introduction into the country, purchase, possession or circulation of counterfeit revenue stamps (Article 459 of the Italian Criminal Code);
Counterfeiting of watermarked paper intended to manufacture public credit instruments or revenue stamps (art. 460 of the Italian Criminal Code);
Manufacture or possession of watermarks or instruments designed for counterfeiting banknotes and coins, revenue stamps or watermarked paper (Article 461 of the Criminal Code);
Use of counterfeit or altered revenue stamps (art. 464 of the Italian Criminal Code)
Counterfeiting, alerting or using of trademarks or distinctive signs, patents, models or designs (Article 473 of the Italian Criminal Code)
Importing and trading in products bearing counterfeit marks (art. 474 of the Italian Criminal Code).

- by virtue of the promulgation and entry into force of the Italian Legislative Decree of 11 April 2002 no. 61 as amended by Law no. 262 of 28 December 2005 and by virtue of the amendments made to the promulgation of Law no. 69 of 27 May 2015 and Italian Legislative Decree no. 38/2017, *the offences set out in art. 25*-ter *of the Decree, i.e. corporate offences*:

False corporate communications (art. 2621, Italian Civil Code); Minor offences (art. 2621 *bis*, Italian Civil Code);
False corporate communications by listed companies (art. 2622, Italian Civil Code);

False statements in a prospectus (art. 2623, Italian Civil Code – art. 173 *bis* Law no. 58 of 24 February 1998)
Falsehood in the reports and communications by audit firms (art. 2624, Italian Civil Code – repealed by art. 37 par. 34 of Italian Legislative Decree no. 39/2010 and replaced by art. 27 of the same decree, entitled: "False reporting or communications by those responsible for statutory auditing";
Obstruction of auditing (art. 2625, Italian Civil Code – par. 1 as amended by art. 37, par. 35 of Italian Legislative Decree no. 39/2010 and referred to in art. 29 of the same decree);
Undue return of contributions (art. 2626 Italian Civil Code); Illegal distribution of profits and reserves (art. 2627 of the Italian Civil Code);
Illegal transactions involving the shares or quotas of the company or its parent company (art. 2628 of the Italian Civil Code);
Transactions to the detriment of creditors (art. 2629 of the Italian Civil Code);
Fictitious capital formation (art. 2632 of the Italian Civil Code);
Improper distribution of company assets by liquidators (art. 2633 of the Italian Civil Code);
Corruption between private individuals (art. 2635 of the Italian Civil Code);
Incitement to corruption between private individuals (art. 2635-*bis* of the Italian Civil Code.)
Unlawful influence on the shareholders' meeting (art. 2636 of the Italian Civil Code);
Stock manipulation (art. 2637 of the Italian Civil Code);
Obstructing the exercise of the functions of public supervisory authorities (art. 2638 of the Italian Civil Code.).

- following the promulgation and entry into force of Law no. 7 of 14 January 2003, the offences set out in art. 25-quater *of the Decree, namely crimes committed for the purpose of terrorism or subverting the democratic order, as defined in the Italian Criminal Code and special legislation*.

- by virtue of the promulgation and entry into force of Law no. 7 of 9 January 2006, *the offences set out in art. 25-quater.1 of the Decree, namely female genital mutilation.*

- by virtue of the promulgation and entry into force of Law no. 228 of 11 August 2003 as amended by Law no. 38 of 6 February 2006 and by Italian Legislative Decree *no. 39 of 4 March 2014, and by Law no. 199/2016, the offences indicated in art. 25*-quinquies *of the Decree, namely crimes against individuals are governed by Section I, Chapter III, Title XII, of Book II of the Italian Criminal Code*.

- following the promulgation and entry into force of Law no. 62 *of 18 April 2005, the offences set out in art. 25-*sexies *of the Decree, namely those relating to market abuse provided for by part V, Title I bis, Chapter II of the Consolidated Law pursuant to Italian Legislative Decree no. 58 of 24 February 1998*:
insider dealing (art. 184 of Italian Legislative Decree no. 58 of 24 February 1998); market manipulation (art. 185 of Italian Legislative Decree no. 58 of 24 February 1998).

- following the promulgation and entry into force of the law on "Ratification and implementation of the United Nations Convention and Protocols Against Transnational Organised Crime adopted by the General Assembly on 15 November 2000 and 31 May 2001", which was definitively approved and published in the Official Journal on 11 April 2006, the *transnational offences referred to in Law no 146 of 16 March 2006*, namely the offences of:
Criminal conspiracy (art. 416 of the Italian Criminal Code); Mafia-type association (art. 416-*bis* of the Italian Criminal Code);
Criminal conspiracy involving the smuggling of manufactured tobacco products (article 291-*quater* of Presidential Decree no. 43 of 23 January 1973);
Criminal conspiracy for the purpose of trafficking in narcotic drugs or psychotropic substances (art. 74 of Presidential Decree no. 309 of 09 October 1990);
Money laundering (art. 648-*bis* of the Italian Criminal Code);
Use of money, goods or benefits of unlawful origin (art. 648-*ter* of the Italian Criminal Code);

Offences relating to the trafficking of migrants, as defined in art. 12 par. 3, 3-*bis*, 3 *ter* and 5 of Italian Legislative Decree no. 286 of 25 July 1998;
Obstruction of justice: inducement not to make statements or to make false statements to judicial authorities (art. 377-*bis* of the Italian Criminal Code);
Obstruction of justice: aiding and abetting (art. 378 of the Italian Criminal Code).

- following the promulgation and entry into force of Law no. 123 of 3 August 2007, the offences provided for by art. 25 septies *committed in violation of accident prevention and occupational health and safety regulations* , namely the crimes of:

Involuntary manslaughter committed in violation of accident prevention and occupational health and safety regulations (art. 589 of the Italian Criminal Code);
Serious and very serious personal injury, committed in violation of accident prevention and occupational health and safety regulations (art. 590 of the Italian Criminal Code).

- following the promulgation and entry into force of Italian Legislative Decree no. 231 of 21 November 2007 as amended by Law no. 186 of 15 December 2014 and Italian Legislative Decree 195/2021, *the offences set out in art. 25*-octies *(Receiving stolen goods, money laundering, using money, goods or benefits of unlawful origin, as well as self-laundering), namely the crimes of:*

Receiving stolen goods (art. 648 Italian Criminal Code);
Money laundering, (art. 648-*bis* Italian Criminal Code);
The use of money, goods or benefits of unlawful origin (art. 648-*ter* of the Italian Criminal Code).
Self-laundering (art. 648 *ter*. 1 of the Italian Criminal Code)

- following the promulgation and entry into force of Law no. 48 of 18 March 2008, *the offences set out in art. 24 bis*, namely cybercrime and unlawful data processing, as amended by Law No. 90/2024:

Unauthorised access to a computer or telecommunications system (art. 615-*ter* of the Italian Criminal Code); unauthorised possession, distribution and installation of devices, codes or other means of accessing computer or telecommunications systems (Art. 615-*quater* of the Italian Criminal Code.)
Illegal interception, obstruction or interruption of computer or electronic communications (art. 617-*quater* of the Italian Criminal Code);
Installation of equipment designed to intercept, prevent or interrupt computer or communication systems (art. 617-*quinquies* of the Italian Criminal Code);
Damage to computer or telecommunications systems (art. 635 *bis* of the Italian Criminal Code.);
Damage to computer information, data and programmes used by the State or another public entity or of public utility (art. 635 *ter* of the Italian Criminal Code);
Damage to computer or telecommunications systems (art. 635-*quater* of the Italian Criminal Code); illegal possession, distribution or installation of computer equipment, devices or programmes designed to damage or disrupt computer or telecommunications systems (Art. 635-*quater.* 1 of the Italian Criminal Code)

Damage to computer or telecommunications systems used by the State or another public entity or of public utility (art. 635 *quinquies* of the Italian Criminal Code); Electronic documents (art. 491 *bis* of the Italian Criminal Code);
Computer fraud by the electronic signature certifier (art. 640-*quinquies* of the Italian Criminal Code).
Violation of the rules on the Cyber National Security Perimeter
Extortion (art. 629, paragraph and of the Italian Criminal Code)

- following the promulgation and entry into force of Law no. 94 of 2009, *the offences set out in art. 24*-ter, namely organised crime:

Criminal conspiracy (art. 416 of the Italian Criminal Code);
Criminal conspiracy to commit one of the offences under articles 600, 601 and 602 of the Italian Criminal Code (art. 416 par. 6 of the Italian Criminal Code);
Mafia-type association (art. 416-*bis* of the Italian Criminal Code); Political-mafia electoral exchange (art. 416-*ter* of the Italian Criminal Code);
Kidnapping for the purpose of extortion (art. 630 of the Criminal Code);
Criminal conspiracy for the purpose of trafficking in narcotic drugs or psychotropic substances (art. 74 of Presidential Decree no. 309 of 9 October 1990).

- following the promulgation and entry into force of Law no. 99 of 2009, *the offences provided for under art. 25*-bis.*1*, namely crimes against industry and commerce:

Interference with the freedom of industry or trade (art. 513 of the Italian Criminal Code);
Unlawful competition involving threats or violence (art. 513 *bis* of the Italian Criminal Code);
Fraud against national industries (art. 514 Italian Criminal Code);
Fraudulent trading (art. 515 Italian Criminal Code);
Sale of non-genuine foodstuffs as genuine (art. 516 of the Italian Criminal Code); Sale of industrial products bearing false or misleading marks (art. 517 of the Italian Criminal Code);
Unlawful manufacture and trade of goods usurping industrial property rights (art. 517-*ter* of the Italian Criminal Code);
Counterfeiting geographical indications or designations of origin of agricultural products and foodstuffs (art. 517 *quater* of the Italian Criminal Code)

- following the promulgation and entry into force of Law no. 99 of 2009, *the offences provided for under art. 25* novies, namely offences relating to copyright infringement:

Art. 171 par. 1 letter a *bis* and 3 Law no. 633 of 22 April 1941 Protection of copyright and other rights related to its exercise;
Art. 171 *bis* Law no. 633 of 22 April 1941;
Art. 171 *ter* Law no. 633 of 22April 1941;
Art. 171 *septies* Law no. 633 of 22 April 1941;
Art 171 *octies* Law no. 633 of 22 April 1941.

- following the promulgation of Law no. 116 3 August 2009, *the offence provided for under art. 25* decies, namely inducement not to make statements or to make false statements to judicial authorities (art. 377 *bis* of the Italian Criminal Code), at national level.

- Following the promulgation of Italian Legislative Decree no. 121 of 7 July 2011 and by the amendments made by Law no. 68 of 22 May 2015, *the offences provided for by art. 25*-undecies, namely. environmental crimes:

Environmental pollution (art. 452 *bis* of the Italian Criminal Code);
Environmental disaster (art. 452 *quater* of the Italian Criminal Code);
Environmental crimes committed through negligence (art. 452-*quinquies* of the Italian Criminal Code);
Trafficking and abandonment of highly radioactive material (art. 452 *sexies* of the Italian Criminal Code);
Killing, destruction, capture, removal, or detention of specimens of protected wild animal or plant species (Article 727-bis of the Italian Criminal Code);
Destruction or deterioration of habitats inside a protected area (art. 733 *bis* of the Italian Criminal Code.);
Articles 137, 256, 257, 258, 259, 260, 260 *bis* and 279 of Italian Legislative Decree n. 152 of 3 April 2006 on the environment; Articles 1, 2 and 3 *bis* Law no. 150 of 7 February 1992 on the Regulation of crimes relating to the application in Italy of the Convention on International Trade in Endangered Species of Wild

Fauna and Flora, signed in Washington on 3 March 1973 pursuant to Law no. 874 of 19 December 1975 and Regulation (EEC) no. 3626/82 and subsequent amendments. These also establish rules for the marketing and detention of live specimens of mammals and reptiles that may pose a danger to public health and safety;
Art. 3 of Law no. 549, of 28 December 1993 Measures to protect the ozone layer and the environment;
Articles 8 and 9 of Italian Legislative Decree no. 202 of 6 November 2007 Implementation of Directive 2005/35/EC on ship-source pollution and consequent sanctions.

- following the promulgation of Italian Legislative Decree no. 109 of 16 July 2012 as amended by Legislative Decree no. 161 of 17 October 2017, *the offences set out in art. 25*-duodecies, relating to the employment of illegal immigrants:

Art. 22 par. 12-*bis* of Italian Legislative Decree no. 286 of 25 July 1998;
Art. 12 par. 3, 3-*bis*, 3-*ter* and 5 of Italian Legislative Decree no. 286 of 25 July 1998.

- following the promulgation of European Law No. 167 of 20 November 2017, *the crimes set out in Article 25*-terdecies relating to racism and xenophobia:

Art. 3 c. 3-*bis*, Law n. 654 of 13 October 1975.

- following the promulgation and of Law no. 39 of 3 May 2019, the offences set out in art. 25-quaterdecies, namely Fraud in sports competitions, illegal gambling or betting, and gambling exercised using prohibited devices:

Articles 1-4 of Law n. 401 of 13 December 1989.

- following the promulgation of Decree Law no. 124 of 26 October 2019, which was subsequently integrated by Legislative Decree no. 75 of 14 July 2020, the crimes set out in art. 25 quinquiesdecies, namely tax offences:

fraudulent tax return through the use of invoices or other documents for non-existent transactions as set out in Article 2, paragraph 1 of Legislative Decree 74/2000;
fraudulent tax return through the use of invoices or other documents for non-existent transactions, as set out in Article 2, paragraph 2-bis of Legislative Decree 74/2000;
fraudulent tax return through the use through other means referred to in Article 3 of Legislative Decree. 74/2000;
issuing invoices or other documents for non-existent transactions pursuant to Article 8, paragraph 1, of Legislative Decree 74/2000;
issuing invoices or other documents relating to non-existent transactions pursuant to Article 8, paragraph 2-bis of Legislative Decree 74/2000;
concealment or destruction of accounting documents pursuant to Article 10 of Legislative Decree no. 74/2000; fraudulent subtraction from the payment of taxes pursuant to Article 11 of Italian Legislative Decree no. 74/2000;
false tax return (art. 4 Legislative Decree no. 74/2000);
failure to file a tax return (art. 5 of Italian Legislative Decree no. 74/2000);
undue compensation (art. 10 quater of Italian Legislative Decree no. 74/2000)

– following the promulgation of Italian Legislative Decree no. 75 of 14 July 2020, as amended by Legislative Decree no. 141/2024, *the crimes set out in Article 25* sexiesdecies, namely smuggling offences:

Smuggling due to failure to declare (art. 78 of Italian Legislative Decree no. 141/2024)
Smuggling by unfaithful declaration (art. 79 of Italian Legislative Decree no. 141/2024)
Smuggling of goods by sea, air and border lakes (art. 80 of Italian Legislative Decree no. 141/2024)
Smuggling involving the improper use of goods imported with a total or partial reduction in duties (art. 81 of Legislative Decree no. 141/2024)
Smuggling in the export of goods eligible for a duty refund (art.82 of Italian Legislative Decree no. 141/2024)

Smuggling relating to temporary export and special use and processing regimes (art. 83 of Legislative Decree no. 141/2024)
Smuggling of manufactured tobacco products (art. 84 of Legislative Decree no. 141/2024);
Aggravating circumstances for the smuggling of processed tobacco products (art. 85 of Legislative Decree no. 141/2024) Criminal conspiracy for the purpose of smuggling of manufactured tobacco products (art. 86 of Legislative Decree no. 141/2024) "Equation of attempted crime to completed crime" (art. 87 of Legislative Decree no. 141/2024).
Aggravating circumstances of smuggling (art. 88 of Legislative Decree no. 141/2024)
Evasion of assessment or payment of excise duty on energy products (Article 40 of Legislative Decree No. 504/1995)
Evasion of assessment or payment of excise duty on manufactured tobacco products (art. 40-bis of Italian Legislative Decree no. 504/1995)
Clandestine manufacturing of alcohol and alcoholic beverages (Article 41 of Italian Legislative Decree no. 504/1995)
Criminal conspiracy for the purpose of clandestine manufacture of alcohol and alcoholic beverages (art. 42 of Italian Legislative Decree no. 504/1995)
Evasion of assessment and payment of excise duty on alcohol and alcoholic beverages (art. 43 of Italian Legislative Decree no. 504/1995)
Aggravating circumstances (art. 45 of Italian Legislative Decree no. 504/1995)
Alteration of devices, stamps and marks (art. 46 of Italian Legislative Decree no. 504/1995).

- following the promulgation of Legislative Decree no. 184 of 18 November 2021 and subsequent amendments by Legislative Decree no. 195 of 18 November 2021, Law no. 137/2023, and Legislative Decree no. 19/2024, the offences set out in art. 25-octies.1, namely crimes relating to non-cash payment means of payment

improper use and counterfeiting of payment cards, credit cards and non-cash payment instruments (Article 493-ter of the Italian Criminal Code), as well as the possession and distribution of equipment, devices or computer programmes designed for use in such crimes (Article 493-quater of the Italian Criminal Code);
computer fraud (art. 640-ter of the Italian Criminal Code).
fraudulent transfer of assets (art. 512 bis of the Italian Criminal Code)

- pursuant to Law No. 22 of 9 March 2022, which contains provisions regarding crimes against cultural heritage and pursuant to art. 25 septiesdecies of Italian Legislative Decree No. 231/2001, namely:

art. 518-bis of the Italian Criminal Code. "Theft of cultural property"
art. 518-ter of the Italian Criminal Code."Misappropriation of cultural property"
art. 518-quater of the Italian Criminal Code "Receiving of cultural property"
art. 518-octies of the Italian Criminal Code "Falsification of private documents relating to cultural property"
art. 518-novies of the Italian Criminal Code. "Violations regarding the alienation of cultural property"
art. 518-decies of the Italian Criminal Code "Illicit import of cultural property"
art. 518-undecis of the Italian Criminal Code "Illicit exit or export of cultural property"
art. 518-duodecies of the Italian Criminal Code Destruction, dispersion, deterioration, defacement, defilement, and unlawful use of cultural or landscape assets
art. 518-quaterdecies of the Italian Criminal Code "Counterfeiting of works of art".

- pursuant to Law No. 22 of 9 March 2022, which contains provisions regarding crimes against cultural heritage pursuant to Article 25 duodevicies of Legislative Decree No. 231/2001, namely:

art. 518-sexies of the Italian Criminal Code "Laundering of cultural property"
art. 518-terdecies of the Italian Criminal Code "Devastation and looting of cultural and landscape assets".

1.5. Offences committed abroad

Pursuant to art. 4 of the Decree, the entity may be held liable in Italy for offences committed abroad.
This liability is based on the following conditions:
a) the offence must have been committed abroad by a party with a working relationship with the company; b) the company must have its registered office in the territory of the Italian State;
c) the company may only be held liable in the cases and under the conditions set out in articles 7, 8, 9 and 10 of the Italian Criminal Code. If the law provides for the punishment of a guilty natural person at the request of the Ministry of Justice, the company will only be subject to proceedings if the request is made to it;
d) if the conditions set out in the aforementioned articles of the Criminal Code are met, the company can be held liable unless the state in which the crime was committed takes action against it.
From another perspective, namely that of crimes committed in Italy by entities under foreign law, it is worth bearing in mind that according to case law from the Court of Cassation, 'the entity is liable for the effects of its conduct, just like 'anyone' else' i.e. like a natural person', regardless of its nationality, the location of its headquarters, or where its primary operations are carried out. This applies if the predicate crime was committed in Italy, or if one of the cases in which national jurisdiction exists applies (even in the case of a crime committed abroad), provided that the additional criteria for attributing liability under Articles 5 et seq. of Legislative Decree No. 231/2001 are met. Therefore, for the purposes of Italian judicial jurisdiction, it is irrelevant that the entity's decision-making centre is located abroad, that the organisational breach occurred outside national borders, or that the person committing the offence is a foreign national or resides outside the country. The same applies to where the crime was planned (Cass. pen., sez. VI, 11 February 2020, no. 11626).

1.6. The sanctions

The administrative sanctions for administrative offences resulting from a crime are as follows:

- pecuniary sanctions;
- restrictive sanctions;
- confiscation of assets;
- publication of the sentence.

Pecuniary sanctions is always imposed for administrative offences that result from criminal activity. The court determines the sanction based on the severity of the offence, the Company's level of responsibility, and the steps it has taken to eliminate or mitigate the consequences of the offence, or prevent further offences.

The pecuniary sanction is reduced if:

- the person who committed the offence did so primarily in their own interest or the interest or that of a third party and the company derived no, or minimal, benefit from it;
- the financial damage caused is particularly insignificant;
- the company has fully compensated for the damage and has eliminated the harmful or dangerous consequences of the offence, or has in any case effectively taken steps to do so;
- the company has adopted and implemented an organisational model suitable for preventing crimes of this type.

Restrictive sanctions apply if at least one of the following conditions is met:

- the company has derived a significant profit from a crime committed by one of its employees or executives, and this crime was committed or facilitated due to serious organisational failings;
- in the event of repeated offences.

The main restrictive sanctions are:

- prohibition from carrying out activities;
- suspension or revocation of authorisations, licences or concessions related to the crime;
- prohibition from contracting with the public administration, except for the provision of a public service;
- exclusion from benefits, financing, grants and subsidies, as well as the revocation of any already granted;
- prohibition from advertising goods or services.

Where necessary, multiple restrictive sanctions can be applied.

A conviction always entails the confiscation of the proceeds or profits of the crime, except for any portion that can be returned to the injured party. The rights acquired by third parties acting in good faith remain unaffected. Confiscation can also be carried out on an "equivalent" basis. This means that if confiscation cannot be ordered in relation to the price or profit of the crime, sums of money, goods or other assets equivalent in value to the price or profit of the offence may be confiscated instead.

The publication of the court's decision may be ordered when a restrictive sanction is applied against the Company.

Rather than imposing a restrictive sanction that would result in the company's activities being interrupted, the court orders the company's activities to be continued by a commissioner for a period equal to the duration of the restrictive sanction that would otherwise have been applied, as long as the conditions for doing so are met. This is provided that at least one of the following conditions is met: a) The company performs a public service whose interruption could cause serious harm to the community; or b) Interrupting the company's activity could have significant repercussions for employment, taking into account its size and the financial conditions of the territory in which it is located.
The profits resulting from the continuation of the business are confiscated.

Restrictive sanctions may also be imposed permanently.
A permanent ban on carrying out the business may be imposed if the company has made a significant profit from the offence and has already received a temporary ban on performing its activity at least three times within the last seven years.

Similarly, a permanent ban on contracting with public administrations or advertising goods or services may be imposed if the company has already received the same sanction at least three times within the last seven years.

This can happen if the company or one of its organisational units is consistently used for the sole or primary purpose of enabling or facilitating the offences for which it is liable.

In this context, art. 23 of the Decree, which it covers the crime of “failure to comply with restrictive sanctions”, is also relevant.

This offence occurs when the obligations or prohibitions inherent in a restrictive sanction are violated while carrying out the activities of the entity to which the sanction applies.

Furthermore, if the entity derives a significant profit from the aforementioned offence, different and additional restrictive sanctions may be applied.

For instance, the company could commit a crime if it participates in a public tender despite being subject to a restrictive sanction that prohibits it from contracting with public administrations.

1.7. Restrictive and asset-related precautionary measures

A company subject to proceedings may be subject to a precautionary measure, such as a restrictive sanction or preventive or conservative seizure.

A precautionary restrictive measure, which involves temporarily disqualifying the company, is imposed when: a) there is serious evidence to suggest that the company is liable for an administrative offence resulting from a crime (serious evidence exist when one of the conditions set out art. 13 of Decree is met: company derived a significant profit from the crime committed by one of its employees or by a person in a senior position, and the crime was committed or facilitated by serious organisational failings; in the event of repeat offences; b) when there is well-founded and specific evidence suggesting a concrete risk of crimes of the same nature as the one being prosecuted being committed.

Asset-related precautionary measures are carried out through preventive seizure and conservative attachment. A preventive seizure may be ordered if the price or profit from the crime is attributable to the company, even if there is no substantial evidence of guilt against the company itself.

Conservative attachment may be ordered in relation to the company's movable or immovable assets, as well as sums or items owed to it, if there is reasonable cause to believe that guarantees for the payment of pecuniary sanctions, the costs of proceedings and other sums owed to the State Treasury are missing or lost.

In this context, art. 23 of the Decree, which it covers the crime of “failure to comply with restrictive sanctions”, is also relevant.

This offence occurs when the obligations or prohibitions inherent in a precautionary restrictive measure are violated while carrying out the activities of the entity to which the measure applies.

Furthermore, if the entity derives a significant profit from the aforementioned offence, different and additional restrictive measures applied may be applied.

For instance, the company could commit a crime if it participates in a public tender despite being subject to a precautionary restrictive measure that prohibits it from contracting with public administrations.

1.8. Actions exempting administrative liability

Art. 6 par. 1 of the Decree provides a specific form of exemption from administrative liability when the offence is committed by individuals in “senior management positions” and the company can prove that:
the governing body adopted and effectively implemented a model suitable for preventing the type of offence that occurred prior to the unlawful act being committed;
it entrusted an internal body, known as the Supervisory Body, with autonomous powers of initiative and control, with the task of overseeing the functioning of the Model and ensuring its compliance and updating;
the individuals in “senior management positions” committed the offence by fraudulently
circumventing the model; there was no lack of oversight or inadequate control by Supervisory Body.

Art. 6 par. 2 of the Decree also stipulates that the model must meet the following requirements:

- identify corporate risks, i.e. activities in which offences may be committed;
- prevent any person working within the company from justifying their conduct by citing ignorance of company regulations, and prevent offences from being caused by errors, including negligence or inexperience, in the assessment of corporate directives;
- introduce a disciplinary system suitable for sanctioning failure to comply with the measures indicated in the model;
- identify ways of managing financial resources that prevent such offences from being committed;
- establish a system of preventive controls that can only be circumvented intentionally;
- establish reporting obligations to the Supervisory Body responsible for monitoring the functioning of, and compliance, with the model.

Art. 6, par. 2 *bis* of the Decree – introduced by Law No. 179 of 30 November 2017 (*Whistleblowing)* – requires the model to include:

- one or more channels through which the persons referred to in Article 5, paragraph 1, letters a) and b), can submit detailed reports of unlawful conduct relevant to the Decree. These reports must be based on precise and consistent facts, or violations of the entity's organisational and management model of which the reporting party has become aware while performing their duties. The aim is to protect the entity's integrity. These channels through guarantee the confidentiality of the reporting party's identity when managing the report;
- at least one alternative reporting channel that guarantees the confidentiality of the whistleblower's identity via electronic means.
- the prohibition of direct or indirect retaliatory or discriminatory acts, direct or indirect, against the whistleblower for reasons directly or indirectly related to the report.

In the disciplinary system adopted in accordance with paragraph 2, letter e), sanctions will be imposed on individuals who violate the protection measures for whistleblowers, as well as on those who intentionally or negligently submit unfounded reports.
Article 7 of the Decree provides for a specific exemption from administrative liability when the offence was committed by “subordinates", provided it is ascertained that company had adopted a suitable model for preventing offences of the same type as the one that occurred, prior to the crime being committed.

In practical terms, to be exempt from administrative liability, the company must:

- adopt a Code of Ethics that establishes the principles of conduct relating to the types of offence;
- establish an organisational structure capable of ensuring a clear and systematic assignment of duties, implementing separation of functions, and encouraging and monitoring correct behaviour;
- formalise manual and IT company procedures to regulate the activity performance. The "segregation of duties" among those carrying out crucial phases of a high-risk process is a particularly effective control tool for preventing this;

- assign authorisation and signature powers consistent with the defined organisational and management responsibilities;
- communicate the Code of Ethics, company procedures, sanctions system, authorisation and signature powers, and all other appropriate tools to prevent the commission of illegal acts to staff in a comprehensive, effective, clear and detailed manner;
- establish an appropriate sanctions system;
- establish a Supervisory Body characterised by substantial autonomy and independence, whose members possess the necessary professional expertise to fulfil their duties;
- establish a Supervisory Body capable of assessing the adequacy of the model, monitor its operation, ensure it is kept up to date, and act with continuity and in close connection with company functions.

2. HISTORY AND PRESENTATION OF THE COMPANY

2.1. Brief background and organisation

Dierre designs, manufactures and markets technologically advanced components and guards with high aesthetic impact for industrial automation in a variety of sectors, including food, ceramics, automotive, pharmaceutical, nautical and electronics.
The company's experience, creative design and passion for research come together to create Profiles, Perimeter and Modular Protections, Linear Guides, Conveyor Lines, Cartesian and Anthropomorphic Robots, Industrial Soundproofing, Protection Systems and Operator Stations. These products are the most efficient and innovative in Europe. In a very short time, Dierre has reinvented itself by creating a network of companies united by a passion for quality and excellence. This has strengthened Dierre's position as market leader in Italy and Germany.

Facilities and offices

DIERRE HEADQUARTERS
At the heart of the Group's core business, Dierre specialises in a wide range of high-quality, durable aluminium sections (more than 300 different types) and maintains a well-stocked central warehouse for the benefit of customers and all Group facilities.
In addition to the cutting and machining of aluminium section bars, Dierre designs and manufactures all types of perimeter and modular protections (Eco Line and Fast Line), custom-made frames, conveyor belts and customised booths for machinery. The company also offers a range of applications to assist operators.
Dierre also houses an important Research & Development centre to ensure its customers have access to cutting-edge solutions for custom-made, efficient, and safe products.

DIERRE MACAP
Thanks to its extensive experience in the field of machine on-board protection, the company designs and manufactures all types of modular accident prevention systems. These offer a complete range of application possibilities for all types of automatic industrial machinery.
Made from various aluminium profiles, these safety guards combine functionality with aesthetic design, becoming an integral part of the machine. They can be calendered to blend in with the surrounding work environment and comply with all international safety regulations.

DIERRE MOTION
Based in Bologna, at the heart of the Packaging Valley, the company designs and manufactures linear units and systems for industrial automation. The company offers a wide range of standard solutions, including more than 20 sizes of extruded parts, linear motion systems with recirculating ball carriages or profiled wheels, and toothed belt or recirculating ball screw drive systems.

DIERRE LECCO
The company offers both standard and customised solutions for the machining of section bars, as well as a complete range of related accessories. The company designs and manufactures light carpentry structures, including frames, perimeter guards and machine on-board protections to prevent accidents. It also produces belt, toothed belt, chain and slat conveyor systems as well as idle and motor-driven roller conveyors. The company also produces welding machines for multiwall polycarbonate sheets as well as related hot and cold blade cutters. It also manufactures machines and lines for industrial automation.

DIERRE LOGISTICS HUB
A new, large Logistics Hub for the entire Group, serving as a warehouse for aluminium profiles and related accessories. Equipped with automatic compactable warehouses and the latest generation of cutting lines, the logistics hub will serve as the base for the new e-commerce service selling aluminium profiles in bundles, loose and cut to size.

DIERRE PRATO
The company specialises in the machining and marketing of profiles and related accessories. It designs and manufactures perimeter and machine on-board protections, as well as aluminium structures - either bare or complete with polycarbonate panels and meshes. It also offers custom-made conveyor solutions with belt and toothed belt drive systems, as well as idle and motor-driven roller conveyors. Customised polycarbonate and methacrylate panels are also available with hot or cold bending options.

DIERRE PADUA
Borgoricco facility This facility is specialises in supplying and machining of high-quality, durable aluminium profiles, as well as perimeter guards and modular guards of all types. It designs and manufactures customised solutions for operators, including workbenches, ladders, gangways, machine frames, and handling systems for transparent and coloured polycarbonate panels. It also designs and manufactures hybrid enclosures by combining its experience in aluminium profile machining with painted steel or iron components to create functional designer-quality products.

DIERRE VICENZA
This facility specialises in the processing of plastic materials, including polycarbonates, methacrylates and all technopolymers. Drawing on its staff's thirty years of experience, the facility offers services such as polished edge laser cutting, hot bending, thermoforming, structural bonding and 5-axis machining.

DIERRE TOOLS
Based in Ferrara, Dierre Tools performs precision CNC milling of aluminium alloys for the Group's various factories. This process enables the Group to reduce production times while maintaining the high quality of its products.
The 600 m2 facility houses three vertical 3-axis machining centres, a tool presetting area and a control room.

DIERRE SAFE
The company designs and manufactures perimeter protection systems including the OMEGA Line, which uses folded mesh, and the EASY Line, which uses framed panels. All products are modular, effective, and compliant with EU (EN) and international (ISO) directives. The company specialises in Door Kits that are designed to provide safe access to work areas by eliminating potentially dangerous elements, such as sharp protrusions and obstructions in passageways. A wide range of panels is available to fit all standard access points, with space for accessories such as locks and brackets for safety devices.

Group companies

SINTESI - a company of Dierre Group
The company provides a comprehensive range of products and services related to the design, prototyping, engineering and industrialisation of customised soundproofing solutions, industrial protection solutions, control rooms and pulpits. It offers reliable and efficient after-sales assistance throughout the production and assembly

process. Sintesi's products and services are characterised by a constant search for the highest level of technology, functionality and design. The company guarantees its customers innovative, aesthetically refined, modern and unique industrial protections and soundproofing solutions.

IN.ECOSISTEMI - a company of Dierre Group
The company offers standard and customisable industrial soundproofing solutions that provide excellent levels of noise reduction for both individual machines and complete systems alike. In addition to industrial safety guards, which ensure compliance with all applicable safety regulations, the company designs and builds control rooms and operator stations. These are designed to create the right working environment while addressing the needs of the internal microclimate, providing peace of mind for employees and contractors alike.

Werden – a company of Dierre Group
The company designs and manufactures protective enclosures for machine tools and medium-light carpentry, providing a comprehensive service. Extensive experience, expertise and cutting-edge technology enable us to create each product from design to assembly and final testing, meeting the precise needs of our customers. High-quality laser cutting, bending and welding processes, combined with meticulous attention to detail throughout the entire production and management processes, prioritise customer satisfaction and loyalty.

2.2. Governance structure

PARENT COMPANY
Dierre S.p.a.
Registered Office: Fiorano Modenese, district Spezzano, via Circond. S.G. Evangelista, n. 23

Corporate structure

omissis

For further information, please refer to the company's internal documents.

Events involving
Dierre *omissis*

3. PURPOSE

To ensure fairness and transparency in its business and corporate activities, the company has adopted a model that complies with Italian Legislative Decree no. 231 of 2001.

The model describes the operating methods employed and the responsibilities assigned within Dierre S.p.a.

As well as being a legal requirement, the company believes that adopting this model is an effective way of raising awareness and keeping all employees and other stakeholders (consultants, partners, etc.) informed.

The Model's objectives are therefore to:

- prevent and reasonably limit the possible risks associated with company activities, with particular attention to risks associated with illegal conduct;
- ensure that all individuals operating in the name of and on behalf of Dierre in high-risk areas are aware that they could commit a crime punishable by criminal and/or administrative sanctions if they violate the provisions of the Model, and that these sanctions could also be imposed on Dierre;
- reiterate that Dierre does not tolerate unlawful behaviour;
- make stakeholders aware of the serious consequences that could arise for the company (and therefore indirectly for them all) from the application of pecuniary and restrictive sanctions provided for by the Decree, and of the possibility that these could be imposed as precautionary measures;
- allow the company to constantly monitor and carefully supervise activities so that it can intervene promptly in risk situations arise and apply the disciplinary measures provided for by the Model, if necessary.

4. SCOPE OF APPLICATION

The rules set out in the Model apply to individuals performing management, administrative, directional or control functions within the company. This includes members and employees, whether formally appointed or not. These rules also apply to individuals who act on behalf of the company or who are contractually bound to it.

The following will be recipients of the model individuals in senior positions: 1) the chairman of the Board of Directors 2) directors; 3) executives; 4) auditors; 5) members of the Supervisory Body; individuals reporting to management: 1) employees; 2) interns.

Specific contractual clauses relating to sensitive activities in these parties participate, may impose specific obligations on the following external parties that are instrumental to the adequate execution of internal control activities provided for in this General Section:

- collaborators, agents, representatives, consultants and, in general, individuals performing self-employed activities, provided they operate in sensitive areas on behalf of, or in the interests of the company;
- suppliers and commercial partners (including temporary company associations and joint ventures) who operate in a significant and/or continuous manner within the so-called sensitive business areas on behalf of, or in the interests of the company.

'External parties' also include individuals or entities that, despite having a contractual relationship with another company within the Group, essentially operate in a significant and/or continuous manner within sensitive business areas on behalf of or in the interests of the company.

Dierre distributes this model using methods that ensure all interested parties are aware of it.

The parties to whom the Model is addressed are required to comply strictly with all its provisions, including the duties of loyalty, fairness, and diligence arising from legal relationships with the Company.

Dierre condemns any conduct that violates the law, and most importantly for our purposes, deviates from the Model and Code of Ethics. This applies even when unlawful conduct is committed in the company's interest or with the intention of gaining an advantage.

5. RISK ASSESSMENT AT DIERRE - UPDATE

5.1. Summary of the project for the preparation and development of the Organisation, Management and Control Model, in accordance with Italian Legislative Decree 231/2001 for Dierre

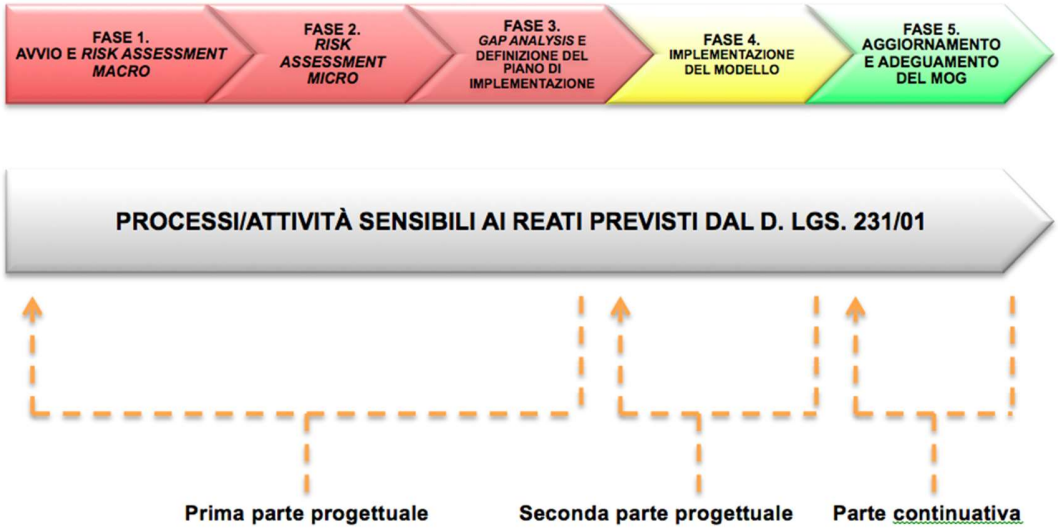
In a meeting on 24 March 2016, Working Group 231 presented the company with the launch of a project aimed at developing the company's Organisation, Management and Control Model (hereinafter referred to as the "OMCM"), pursuant to art. 6, par. 2, *a)* of Italian Legislative Decree 231/01 and the Confindustria Guidelines.

The OMCM was developed for Dierre S.p.A., with registered office in Fiorano Modenese, Spezzano district, Via Circond. S. G. Evangelista, 23.

Throughout the project, "Working Group 231" involved the relevant company functions to a large extent in understanding, analysing, and evaluating the various topics, as well as sharing information. This was done through meetings and interviews aimed at gathering information and at conducting a detailed risk area analysis and assessment. Periodic reports were also produced on the project's progress and any critical issues that emerged.

The OMCM preparation and development project involved the following steps and was completed in 4 months (March 2016 – July 2016).

Figure 1: Dierre organisation, management and control model



5.2. Stage 1: Start and Macro Risk Assessment

This stage involved the following activities:

- Organisation, planning, announcement and start of the OMCM preparation and development project;
- Gathering of preliminary documentation/information;
- Company analysis and identification of risk areas pursuant to Italian Legislative Decree 231/01 ("macro areas" of sensitive activities) and the relevant company managers/roles involved;

- Analysis and assessment of Dierre's control environment to identify any gaps with respect to key components of the OMCM.

The next stage involved producing specific planning, organisational, communication, and project launch documentation for the preparation and development of the OMCM.

5.3. Stage 2: Micro Risk Assessment

This stage involved the following activities:

- Detailed analysis of risk areas identified through interviews;
- Identification of specific processes/activities sensitive to the crimes envisaged by Italian Legislative Decree 231/01, which that emerged from the detailed analysis of the areas ("macro areas" of sensitive activities);
- Risk assessment by mapping sensitive processes in terms of:
- foreseeable and abstractly hypothetical offences to which each process is exposed;
  - potential ways in which the offence could be carried out for each process;
  - organisational functions/company roles involved in the process;
  - level of cover – through preventive protocols – for processes in terms of: system of powers, information systems, documentary procedures and reporting;
  - description of the process flow.

The process mapping is included in this "General Section" and in the individual "Special Sections" of the Organisation, Management and Control Model.

5.4. Stage 3: Gap Analysis and establishing the implementation plan

This stage involved the following activities:

- Identification of the framework of preventive protocols (system-wide and specific) to be applied to each sensitive process ("macro areas" of sensitive activities) to prevent offences under Italian Legislative Decree 231/01 and subsequent amendments from being committed;
- Assessment of the mapping of sensitive processes – carried out in Stage 2 – to identify shortcomings in sensitive processes with respect to the identified preventive protocol framework (*Gap Analysis*);
- Definition of the action plan to be implemented for the development of the OMCM within the company, taking into account the shortcomings that emerged in the processes (*Micro Risk Assessment*) and the recommendations relating to the control environment and the macro components of the model (*Macro Risk Assessment*) made in Stage 1 of the project.

The outcome of these activities is reported in this "General Section" and in the individual "Special Sections" of the Organisation, Management and Control Model.

5.5. Stage 4: Implementation of the organisation, management and control model for Dierre

This stage involved the following activities:

- Implementation of the improvement action plan – defined in Stage 3 – which led to the definition, sharing and formalisation of:

- macro components of the OMCM: Code of Ethics, Organisational Structure, System of Delegations and Powers, Sanctions System, Supervisory Body regulations;
- preventive protocols - system-wide and specific - and support processes for each "macro area" of sensitive activity, subject to detailed analysis in the relevant "Special Sections".

- Formalisation of the organisation, management and control model pursuant to Italian Legislative Decree 231/01, which is reproduced in full in the attachment to this document.

The Organisation, Management and Control Model pursuant to Italian Legislative Decree 231/01 was presented to senior management and subsequently submitted to the company's Board of Directors. The Board approved the initial version of the model in a resolution.

5.6. Stage 5: Updating and adapting the Model to reflect organisational and regulatory changes

Therefore, risk analysis must be considered a dynamic process, enabling the Supervisory Body and the company as a whole to remain constantly aware of the risk factors involved in their management.
This involves repeating the entire analysis cycle for all company activities and adding legislative changes (e.g. new offences or risk management methods etc.) and process changes resulting from organisational changes and the company's evolution since the last update.
Lastly, the risk profile must be recalculated by applying the model to identify both Inherent and Residual Risk.
During this updating process, it is not necessary to compare current and previous risk profiles, since these refer to organisational and legislative contexts that are not necessarily comparable.
Improvement or corrective actions will therefore be defined based on the updated risk analysis rather than on the differences between risk profiles.
While an overall comparison is not meaningful, the difference in risk associated with one or more activities (whether positive or negative) can help to determine which activities should be undertaken in order to prevent an offence. Evaluating the reasons for a change in the residual risk of a given activity can provide useful insights into the most appropriate areas for intervention.

Updating and adapting the Model 231 is based on the results of the audits conducted by the Supervisory Body, as well as on the needs that emerge from using the Model itself.

With regard to the regulatory update in particular, the update, which dates back to January 2025, focuses on the risks introduced by recent regulatory changes in this area. Specifically:

- Legislative Decree No. 195/2021 concerning the receipt, laundering or use of money, goods or benefits of unlawful origin, as well as self-laundering pursuant to art. 25-*octies* of Legislative Decree no. 231/2001;
- Legislative Decree no. 184/2021, and subsequent amendments made by Legislative Decree no. 195 of 18 November 2021, the offences set out in art. 25-octies.1 relating to non-cash means of payment;
- Law No. 22 of 9 March 2022, containing provisions regarding crimes against cultural heritage pursuant to art. 25 septiesdecies of Legislative Decree No. 231/2001 as well as art. 25 duodevicies of the same decree
- Law no. 137/2023, introduced the offences referred to in Articles 353 and 353-bis of the Italian Criminal Code, as well as the offence referred to in art. 512-bis of the Italian Criminal Code, as amended

by Law Decree no. 19/2024;
- Law no. 90/2024 on Cybersecurity;
- Law no. 112/2024 introduced the crime of misappropriation of money or movable property as set out in art. 314 bis of the Italian Criminal Code;
- Law no. 114/2024 repealed the abuse of office provision under art. 323 of the Italian Criminal Code.
- Italian Legislative Decree no 141/2024 reformed smuggling offences and introduced offences relating to excise duties into Legislative Decree. no. 231/2001;
- Organisational changes relating to corporate mergers and operations involving Dierre Decatche, Dierre Toscana and Dierre Safe.

The Organisation, Management and Control Model pursuant to Italian Legislative Decree 231/01 was presented to senior management and subsequently submitted to the company's Board of Directors. The Board approved the initial version of the model in a resolution.

6. STRUCTURE AND ORGANISATION OF THE MODE

6.1. Reference models

This Model is based on the 'Guidelines for the Construction of Organisation, Management and Control Models pursuant to Legislative Decree 231/01' that were approved by Confindustria on 7 March 2002 and updated in June 2021.

With regard to whistleblowing regulations, the update to the Model draws on Confindustria's explanatory note of January 2018 and Assonime's circular of 28 June 2018. It is also inspired by the ANAC guidelines of July 2023 and Confindustria's operational guide of October 2023.

The key stages identified in the construction of models by the guidelines can be summarised as follows:

- The first stage involves identifying risks by analysing the company context to determine in which areas/sectors of activity events that could harm to the objectives set out in the Decree may occur, and how;
- The second stage involves designing the control system (i.e. protocols for scheduling training and implementing the entity's decisions) and assessing the existing system to identify any necessary adjustments to ensure it can effectively counteract or reduce identified risks to an acceptable level.

Conceptually, risk reduction involves addressing two key factors: 1) the probability of the event occurring and 2) the potential impact of the event itself.

In order to operate effectively, the outlined system must be an ongoing process that pays particular attention to moments of corporate change; it cannot be limited to sporadic activity.

It should also be noted that the basis for establishing an adequate preventive control system hinges on defining "*acceptable risk*".

While risk is generally considered an acceptable part of control system design for protecting against *business* risks when the "cost" of additional controls exceeds the value of the resource being protected, such as ordinary cars being equipped with anti-theft devices rather than armed guards, the economic logic of costs cannot be used as the only reference point in the context of Italian Legislative Decree no. 231 of 2001. In order to apply the provisions of the decree effectively, it is important to define an acceptable threshold that limits the quantity and quality of preventive measures introduced to prevent the offences in question. Furthermore, without first determining an acceptable level of risk, the quantity and quality of preventive controls that could be introduced would be virtually infinite, which would have obvious consequences for corporate operations. Furthermore, the general principle of the concrete enforceability of conduct, summarised in the Latin maxim *ad impossibilia nemo tenetur*, can be invoked in criminal law and is an indispensable reference criterion, even if identifying its exact limit is often difficult in practice.

The above-mentioned notion of 'acceptability' relates to the risks associated with conduct that deviates from the organisational model's rules rather than to underlying work-related health and safety risks. According to the principles of current accident prevention legislation, these risks must be eliminated entirely based on knowledge acquired through technological progress. Where this is not possible, the risks must be minimised and managed.

With regard to the preventive control system to be implemented in relation to the risk of committing offences under Italian Legislative Decree no. 231 of 2001, the conceptual threshold of acceptability for intentional offences is a **prevention system that cannot be circumvented except through fraud.**

This solution aligns with the logic of "fraudulent evasion" of the organisational model which is an express exemption to the aforementioned legislative decree for the purposes of excluding the entity's administrative liability (art. 6, par. 1, *c)*, *"persons committed the offence by* ***fraudulently*** *evading the organisation and management models"*).

By contrast, in cases of involuntary manslaughter or personal injury through negligence, committed in breach of health and safety regulations in the workplace, the conceptual threshold of acceptability for the purposes of exemption under Italian Legislative Decree No. 231 of 2001 is conduct that does not involve an intention to cause death or personal injury and violates the preventive organisational model (and the underlying mandatory requirements of accident prevention legislation). This applies even if the relevant Supervisory Body promptly fulfils the supervisory obligations set out in Italian Legislative Decree No. 231 of 2001. This is because evasion of organisational models through fraud appears to be incompatible with the subjective elements of the crimes of involuntary manslaughter and personal injury due to negligence, as set out in articles 589 and 590 of the Italian Criminal Code.

According to the guidelines, the creation of a risk management system must assume that offences can still be committed even after the model has been implemented. In the case of intentional offences, the model and relevant measures must ensure that the offender not only "intends" to commit the offence (e.g. bribery of a public official) but also that they can only do so by fraudulently circumventing the entity's instructions (e.g. through artifice and/or deception). The set of measures that an offender would be "forced" to take in order to commit an offence must relate specifically to the activities of the entity in question and the offences potentially linked to them. However, in the case of negligent offences, the intention must relate to the conduct, rather than the event itself.

The methodology for creating a risk management system, which is outlined below is generally applicable.
This process can be applied to various types of risk, such as legal, operational and financial *reporting* etc. This feature enables the same approach to be adopted when the principles of Italian Legislative Decree no. 231 of 2001 are extended to other areas. With reference to the extension of Legislative Decree no. 231 of 2001 to include involuntary manslaughter and personal injury through negligence in breach of health and safety regulations in the workplace, it should be reiterated that current legislation on the prevention of work-related risks sets out the essential principles and criteria for managing workplace health and safety. Therefore, in this context, the organisational model must incorporate these prerequisites.

For organisations that already have internal self-assessment procedures in place, including certified ones, the focus should be on applying these procedures to all types of risk using all the methods set out in Legislative Decree no. 231 of 2001. It is worth bearing in mind that risk management is an iterative process that companies must implement internally using whatever methods they deem most appropriate, while ensuring compliance with legal obligations. The models developed and implemented at a corporate level will be based on each entity's documented application of the guidelines provided here, taking into account their internal operating context (organisational structure, territorial distribution, size, etc.) and external context (economic sector, geographic area), as well as offences hypothetically linked to their risk activities.

With regard to operational risk management methods, particularly those entrusted to specific individuals or roles within the company, there are essentially two methodologies:

- assessment by a company body that performs this activity together with line management *management*;
- self-assessment by the operating *management* with support from a methodology tutor/facilitator.

The operational steps that the company must take to implement a risk management system in line with the above logical approach comply with the requirements of Italian Legislative Decree No. 231 of 2001. These requirements are set out below. When describing this logical process, emphasis should be placed on the outcomes of the self-assessment activities carried out to set up the system.

Inventory of company areas of activity

This stage can be carried out using a variety of approaches, such as categorising by activity, by function or by process. It involves carrying out a comprehensive periodic review of the company to identify areas affected by potential offences. With regard to crimes against public administrations, for example, it is necessary to identify areas that, by their very nature, have direct or indirect ties to national and foreign public administrations. Certain types of processes and functions will certainly be affected (e.g., sales to public administrations and management of concessions from local public administrations etc.), while others may not be affected at all or only marginally. However, with regard to homicide and serious or very serious bodily harm committed in violation of occupational health and safety regulations, no area of activity can be ruled out a priori, since these crimes could affect all corporate functions.

As part of the review of at-risk processes and functions, it is important to identify individuals who are subject to monitoring. In exceptional circumstances relating to intentional crimes, this could also include individuals with indirect relationships with the company, such as agents, as well as individuals with relationships with the company, such as commercial partners, their employees and their collaborators.
Regarding involuntary manslaughter and personal injury committed in breach of occupational health and safety regulations, all workers covered by the same legislation are subject to monitoring.

Similarly, *due diligence* should be carried out whenever 'suspicious indicators' relating to a particular commercial transaction are identified during the risk assessment process. Examples of such indicators include negotiations conducted in territories with high corruption rates, overly complex procedures or the presence of new staff who are unknown to the entity.

Lastly, it should be emphasised that each company and sector has its own specific risk areas that can only be identified through a thorough internal analysis. However, financial processes are clearly important for the purposes of applying Italian Legislative Decree no. 231 of 2001.

Analysis of potential risks.

This analysis should consider how offences could be committed within the various business areas outlined in the previous section. The results will form the basis for designing preventive measures and must provide a comprehensive overview of how offences can be committed in relation to the company’s internal and external operating context.

In this regard, it is useful to consider the entity's history, i.e. its past experiences, as well as the characteristics of other entities operating in the same sector, particularly with regard to any offences they have committed in the same line of business.
In particular, analysing the ways in which offences such as murder, bodily harm or serious bodily harm through negligence can be committed in breach of occupational health and safety obligations corresponds to the work-related risk assessment carried out in accordance with the criteria set out in art. 28 of Italian Legislative Decree n. 81 of 2008.

Assessment / creation / adaptation of the preventive control system
The activities described above include assessing any existing preventive control system and adapting it where necessary, or developing it if one does not exist. The preventive control system must ensure that the risk of offences being committed using the methods identified and documented in the previous stage is reduced to an "acceptable level", as defined in the introduction. This essentially involves designing the *"specific protocols to plan the development and implementation of the entity's decisions regarding the crimes to be prevented"* as defined in Italian Legislative Decree no. 231 of 2001. There are numerous components to an internal preventive control system for which there are well-established methodological references.

However, it should be reiterated that the preventive control system must be such that:
- in the case of intentional crimes, it cannot be circumvented except intentionally;
- in the case of negligent offences that are not fraudulent, the system must still be found to have been violated, even if the relevant supervisory body has strictly complied with its supervisory obligations.

According to the information provided, the following are listed as the **components (protocols) of a preventive control system**, which must be implemented at company level to ensure the effectiveness of the model. These components are generally considered to be the intentional and negligent offences provided for by Legislative Decree no. 231 of 2001.

A) **Preventive control systems for intentional crimes**
According to the Guidelines proposed by Confindustria, the most important components of the control system are:

- the Code of Ethics with references to the offences considered;

- a clear, formalised organisational system, especially with regard to the attribution of liability;

- manual and computerised procedures (information systems) to regulate activities by providing appropriate control points. In this context, an effective preventive tool is one that separates the duties between those carrying out crucial stages (activities) of a high-risk process;

- powers of authorisation and signature powers assigned in accordance with the defined organisational and management responsibilities;

- a management control system that can provide timely notification of the existence and the onset of general and/or particular critical situations;

- communication to staff and their training.

B) Preventive control systems to prevent crimes such as involuntary manslaughter and personal resulting from a breach of occupational health and safety regulations

Without prejudice to what has already been specified with regard to intentional offences, the most important components of the control system in this context are:

- the Code of Ethics (or of Conduct) with references to the offences considered;

- an organisational structure with formally defined duties and responsibilities regarding occupational health and safety that are consistent with the company's organisational and functional structure, extending from employer to individual worker. Particular attention should be paid to specific roles in this area.

This approach essentially requires that:

a) the organisational and operational duties of company management, managers, supervisors and workers must explicitly specify safety activities and responsibilities when carrying out these activities;

b) the duties of the Health and Safety Manager, Assistant Health and Safety Manager, Workers' Safety Representative, emergency management personnel and competent doctor must be documented;

- Training: performing tasks that may affect employee health and safety at work requires adequate skills, which must be verified and maintained through training. This ensures that all staff, at all levels, are aware of the importance of complying with the organisational model and the potential consequences of deviating from the rules set out in the model. Specifically, each worker/operator must receive sufficient and appropriate training relating to their own job and duties. This training must be provided when an employee is hired, transferred, or has a change in duties, or when new work equipment, technologies or hazardous substances and preparations are introduced. The company should organise training according to periodically identified needs;

- communication and engagement: circulating information within the company is important for fostering the involvement of all stakeholders and ensuring adequate awareness and engagement at all levels. Engagement should be achieved through:

a) prior consultation regarding the identification and assessment and the definition of preventive measures;

b) periodic meetings that take into account at least the requirements set out in current legislation, including meetings scheduled for company management.

- Operational management: the occupational health and safety risk control system should be integrated into, and consistent with, the company’s overall management of processes. Analysing company processes and their interrelationships, together with the results of the risk assessment, helps determine how activities that significantly impact occupational health and safety should be carried out safely. Once the relevant health and safety intervention areas have been identified, the company should ensure that their operational management is properly regulated.

In this regard, particular attention should be paid to the following:

a) the hiring and qualifications of staff;

b) the organisation of work and workstations;
c) the acquisition of goods and services used by the company and the communication of necessary information to suppliers and contractors;
d) regular and extraordinary maintenance;
e) the qualification and selection of suppliers and
contractors; f) emergency management;
g) procedures for addressing discrepancies between the set objectives and the rules of the control system;

Safety monitoring system: Occupational health and safety management should include a stage to verify that risk prevention and protection measures adopted and deemed appropriate and effective are being maintained. The technical, organisational and procedural prevention and protection measures implemented by the company should be subject to scheduled monitoring.
A monitoring plan should be prepared and include:
a) scheduling of checks (frequency);
b) allocation of duties and executive responsibilities;
c) description of methodologies to be followed;
d) methods for reporting any non-compliant situations.

Provisions for systematic monitoring should therefore be made, and the methods and responsibilities should be established at the same time as those for operational management.

This **first-level monitoring** is generally carried out by internal company resources, either through self-monitoring by the operator or by the supervisor/manager. However, specialised aspects (e.g. specialised audits) may involve the use of other resources, either inside or outside the company. Ideally, verification of organisational and procedural measures relating to health and safety should be carried out by individuals to whom responsibilities have already been assigned (usually managers and supervisors). The Prevention and Protection Service plays a particularly important role in this, as it is responsible for developing control systems for the measures adopted within its area of expertise.

The company must also periodically conduct **second-level monitoring** of the functionality of the adopted preventive system. Functionality monitoring should inform strategic decision-making and be conducted by competent staff who can guarantee their work is objective, impartial and independent of the area being inspected.

According to the Confindustria Guidelines, the components described above must be seamlessly integrate into a system architecture that complies with a series of control principles, including:

- *every operation, transaction and action must be verifiable, documented, consistent and appropriate*. Supporting documentation must be available at any time to verify the reasons for and characteristics of each action, as well as identifying who authorised, performed, recorded, and verified it;
- *no-one can manage an entire process independently*: the system must guarantee the application of the separation of duties principle, whereby authorisation to carry out a transaction is the responsibility of someone other than the person performing, monitoring or keeping the accounting records for the operation;
- *control records:*: the control system must document the performance of controls and supervision (possibly through the production of minutes);

It should be noted that failure to comply with specific points of the Confindustria Guidelines does not affect the validity of the Model. In fact, as each model must be drafted with specific consideration of the company's circumstances, it may be necessary to deviate from the Guidelines to ensure compliance with the Decree's requirements. As the guidelines are general by nature, this deviation is to be expected.

Accordingly, the *case study* and the summary list of control instruments set out in the appendix to the Guidelines should also be evaluated.

C) Preventive control systems for environmental crimes

Without prejudice to what has already been specified with regard to intentional offences, the most important components of the control system in this context are:

- the Code of Ethics (or of Conduct) with references to the offences considered;

- an organisational structure with formally defined environmental duties and responsibilities, that are consistent with the company's organisational and functional structure, extending from the legal representative to the individual worker. Particular attention should be paid to specific roles in this area.

This approach essentially requires that:

a) the organisational and operational duties of company management, managers, supervisors and workers must explicitly specify those relating to environmental activities for which assigned to them, as well as the associated responsibilities;
b) the duties of the Environmental Management System Manager, including external ones, are documented;

- information and training: performing tasks that may affect employee profiles requires the right skills, which must be verified and maintained through training. This ensures that all staff, at all levels, understand the importance of complying with the organisational model and recognise potential consequences of behaviour that deviates from the rules set out in the model. Specifically, all individuals involved must receive sufficient and appropriate training relating to their own job and duties. This training must be provided when an employee is hired, transferred, or has a change in duties, or when new work equipment, technologies or hazardous substances and preparations are introduced. The company should organise training according to periodically identified needs, documenting it with clear records of the course contents, mandatory participation and the attendance checks. These documents must be retained.

- communication and engagement: circulating information within the company is important for fostering the involvement of all stakeholders and ensuring adequate awareness and engagement at all levels. Engagement should be achieved through:
  a) prior consultation regarding the identification and assessment and the definition of preventive measures;
  b) periodic meetings that take into account at least the requirements set out in current legislation, including meetings scheduled for company management;

- operational management: the control system relating to environmental risks should be integrated into, and consistent with, the company's overall management of processes.

In this regard, particular attention should be paid to the following:

a) the hiring and qualifications of staff;
b) the organisation of work and workstations;
c) the acquisition of goods and services used by the company and the communication of necessary information to suppliers and contractors;
d) regular and extraordinary maintenance;
e) the qualification and selection of suppliers and contractors;
f) procedures for addressing discrepancies between the set objectives and the rules of the control system.

- Environmental profile monitoring system: environmental protection management should include a stage for verifying the maintenance of risk prevention and protection measures that have been deemed suitable and effective. The technical, organisational and procedural prevention and protection measures implemented by the company should be subject to scheduled monitoring.

A monitoring plan should be prepared and include:

a) scheduling of checks (frequency);
b) allocation of duties and executive responsibilities;
c) description of methodologies to be followed;
d) methods for reporting any non-compliant situations.

Provisions for systematic monitoring should therefore be made, and the methods and responsibilities should be established at the same time as those for operational management.

This **first-level monitoring** is generally carried out by internal company resources, either through self-monitoring by the operator or by the supervisor/manager. However, specialised aspects (e.g. specialised audits) may involve the use of other resources, either inside or outside the company. Ideally, verification of organisational and procedural measures relating to environmental protection should be carried out by individuals to whom responsibilities have already been assigned.

The company must also periodically conduct **second-level monitoring** of the functionality of the adopted preventive system. Functionality monitoring should inform strategic decision-making and be conducted by competent staff who can guarantee their work is objective, impartial and independent of the area being inspected.

The components described above must seamlessly integrate into a system architecture that complies with a series of control principles, including:

- every operation, transaction and action must be verifiable, documented, consistent and appropriate. Supporting documentation must be available at any time to verify the reasons for and characteristics of each action, as well as identifying who authorised, performed, recorded, and verified it;
- no-one can manage an entire process independently: the system must guarantee the application of the separation of duties principle, whereby authorisation to carry out a transaction is the responsibility of someone other than the person performing, monitoring or keeping the accounting records for the operation;

- control records: the control system must document the performance of controls and supervision (possibly through the production of minutes).

6.2. Framework and approval rules for the Model and its updates

The methodology used to prepare the Model was consistent with that proposed by the Confindustria Guidelines:

- identifying so-called *sensitive* activities through a preliminary examination of company documentation (e.g. articles of association, regulations, organisational charts, powers of attorney, assignments, organisational provisions and communications) as well as a series of interviews with individuals responsible for different business operations (i.e. department managers). This analysis aimed to identify and evaluate activities and their performance that could constitute unlawful conduct and potentially lead to predicate offences being committed. At the same time, existing control measures, including preventive ones, were assessed, as were any critical issues requiring improvement;

- planning and implementing the necessary actions to improve the control system and adapt it to the aims of the Decree, taking into account the Confindustria Guidelines and the fundamental principles of separation of duties as well as defining authorising powers in line with assigned responsibilities. Particular attention was paid to identifying and regulating the financial management and control processes involved in high-risk activities during this stage;

- defining control protocols where an existing risk had been identified. Decision-making and implementation protocols have been defined. These protocols set out the rules and procedures agreed by those responsible for the operational management of these activities as being the most suitable for managing the identified risk profile. When developing the control system, the principle adopted is that the conceptual threshold of acceptability is represented by a prevention system that cannot be circumvented except through fraud, as already indicated in the guidelines proposed by Confindustria. The protocols are based on the principle of documenting and verifying the various stages of the decision-making process, enabling the rationale behind the decision to be traced.

The key parts of the Model are therefore:
- mapping the company's activities at risk, i.e. activities in which offences under the Decree could be committed;
- providing appropriate monitoring sessions to prevent offences under the Decree from being committed;
- *ex post* verification of corporate behaviour and the functioning of the Model with consequent periodic updating;
- the dissemination and involvement of all business levels in implementing behavioural rules and established procedures;
- assigning specific supervisory duties relating to the effective and correct functioning of the Model to the Supervisory Body; - creating a Code of Ethics.

Without prejudice to the specific purposes described above and in relation to the exemption provided for by the Decree, the Model forms part of the broader existing control system. This system is designed to provide reasonable assurance that corporate objectives will be achieved in compliance with laws and regulations, that financial information will be reliable and that assets will be protected, including against potential fraud.

With reference to *sensitive* areas of activity in particular, the company has identified the following core principles of the model. These principles govern such activities, serving as the tools used to plan, prepare and implement company decisions, while ensuring proper control and preventing offences:
- separation of duties through the correct distribution of responsibilities and adequate authorisation levels. This aims to avoid functional overlaps or operational assignments that focus critical activities on one individual;
- clear and formalised assignment of powers and responsibilities, with explicit indications of the limits of their exercise, consistent with the duties assigned and positions held within the organisational structure;
- no significant operation can be undertaken without authorisation;
- the existence of appropriate rules of conduct to ensure that the company's activities are conducted in accordance with laws and regulations, and that its assets are protected;
- adequate procedural regulation of *sensitive* corporate activities is in place to ensure that: operational processes are defined and adequately documented so that they can be verified in terms of fairness, consistency and accountability at any time; operational choices and decisions are always traceable in terms of characteristics and motivations, and those who have authorised, performed and verified individual activities can always be identified; the management of financial resources is guaranteed to prevent offences being committed; supervision and monitoring activities on business transactions are carried out and documented; security mechanisms ensure adequate protection for physical and logical access to data and company assets; information exchanged between consecutive stages or processes ensures the integrity and completeness of the managed data.

These principles are consistent with the indications provided in the Confindustria Guidelines and are considered effective in preventing the offences referred to in the Decree.

The company therefore believes it is essential to ensure the correct and specific application of the aforementioned control principles in all *sensitive* areas of company activity, as indicated and described in the Special Sections of this Model.

6.3. Basis and content of the model

The Model prepared by Dierre is based on:
- the Code of Ethics, which establishes general behavioural guidelines;
- the organisational structure, which defines the assignment of duties and provides for the separation of functions, where possible, or compensatory controls - and identifies the individuals responsible for ensuring correct conduct;
- the mapping of sensitive business areas, i.e. the description of the processes in which offences are most likely to be committed;
- support processes for sensitive corporate areas, i.e. processes used to manage financial instruments and/or alternative means that could facilitate offences being committed in high-risk areas;
- the use of formalised company procedures aimed at regulating the correct operating procedures for making and implementing decisions in the various sensitive business areas;
- the details of the individuals responsible for such activities, ideally with executors and controllers in different roles, in order to separate management and control duties;
- the adoption of a system of delegations and powers consistent with the assigned responsibilities, ensuring a clear and transparent representation of the corporate decision-making and implementation process in accordance with the requirement for one person to be in charge of the function;

- the identification of methodologies and tools that ensure an adequate level of direct and indirect monitoring and control. The first type of control is entrusted to operators and manager of a given activity, while the second type is entrusted to management and the Supervisory Body;
- the specification of information formats for monitoring and control activity traceability (e.g. forms spreadsheets, reports, etc.);
- the reporting procedure is designed to protect the entity from unlawful conduct pursuant to Legislative Decree no. 231/2001, as well as from violations of its organisational and management model. The procedure ensures the confidentiality of the whistleblower's identity throughout the management of the report. This includes implementing at least one alternative reporting channel that guarantees the confidentiality of the whistleblower's identity via electronic means;
- the definition of a disciplinary system for those who violate the company's rules of conduct. This system, on the one hand, must include a prohibition on retaliatory or discriminatory acts, whether direct or indirect, against whistleblowers within the timeframe set out in the whistleblowing procedure, for reasons directly or indirectly related to the report. Furthermore, it must provide sanctions for those who violate protection measures for whistleblowers, as well as for those who intentionally or through gross negligence submit unfounded reports;
- the implementation of a plan for: 1) training executive and managerial staff working in sensitive areas, directors and the Supervisory Body; 2) informing all other interested parties;
- the establishment of a Supervisory Body to oversee the effectiveness, proper functioning and periodic updating of the model, and to ensure its consistency with the objectives.

The documentation relating to the model consists of the following special sections:

Special section	Description
A	Code of ethics
B	Organisational structure and system of delegations
C	Structure, composition, regulations and functioning of the Supervisory Body
D	Sanctions system
E	Offences against the Public Administration and against the State
F	Offences relating to the counterfeiting of legal tender, public credit instruments, revenue stamps and identification tools or signs
G	Corporate offences
H	Offences against the individual
I	Offences relating to workplace safety
J	Offences relating to the receipt, laundering or use of money, goods or benefits of unlawful origin, as well as self-laundering
K	Offences relating to cybercrime and unlawful data processing
L	Offences relating to copyright infringement
M	Crimes against industry and commerce
N	Offences pursuant to Article 377-bis of the Italian Criminal Code
O	Offences relating to organised crime
P	Environmental crimes
Q	Offences related to the employment of illegal immigrants
R	Transnational offences referred to in Italian Law no. 146 of 16 March 2006

S	Tax offences
T	Offences relating to smuggling
U	Offences relating to non-cash means of payment
Compliance manual –	
Reporting procedure	Whistleblowing

6.4. Code of ethics

The Code of Ethics is a document independently developed and adopted by Dierre to inform all parties of the company's principles of corporate ethics, as well as its ethical commitments and responsibilities when conducting business and corporate activities. The company intends to comply with these principles. All Dierre employees and contractors are expected to comply with it.

The principles and rules of conduct contained in this Model align with those set out in the company's Code of Ethics. However, the scope of the model differs from that of the Code itself, as the Model is intended to implement the provisions of the Decree.
It should be noted that the Code of Ethics is an instrument adopted independently by the company and can be applied generally to express its own set of recognised corporate ethics principles. The company intends these principles to be observed by all its employees, as well as by all individuals and organisations that cooperate with it to achieve its business goals, including suppliers and customers. However, the Model responds to specific provisions in the Decree that are aimed at preventing particular types of offences committed in or to the apparent interest advantage of the company, which may result in administrative liability under the provisions of the Decree. Nevertheless, as the Code of Ethics also covers principles of conduct that are suitable for preventing the unlawful conduct referred to in the Decree, it is relevant to the purposes of the Model and formally constitutes an integral part of it.

The company's Code of Ethics can be found in "Special Section A: Code of ethics".

6.5. Organisational structure

The company's organisational structure is defined by the President issuing delegations of functions and organisational provisions, such as service orders, job descriptions, and internal organisational directives.
Both the Model and Dierre's organisational structure will be posted on the Intranet portal.
The Human Resources Manager must also keep the personnel structure up to date and communicate all significant changes to the Supervisory Body.
Dierre's organisational structure forms an integral part of the model and is set out in "Special Section B: Organisational structure and system of delegations". This section illustrates of the company's divisions and the functions assigned to each one.

6.6. Reporting procedure (Whistleblowing)

Law No. 179, containing "Provisions for the protection of those who report crimes or irregularities of which they have become aware in the context of a public or private employment relationship", came into force on 29 December 2017.
The law aims to encourage workers to help expose corruption within public and private organisations.

With regard to the private sector, Article 2 of Law No. 179/17 amends Decree 231 by adding a new provision into Article 6 ("Senior management and organisational models"), which includes measures relating to the submission and management of reports within the scope of Model 231.
Consequently, the law requires companies that adopt the Model to implement these new measures.
In particular, Model 231 must include the following additional measures to be considered suitable and effective:

- one or more channels through which individuals referred to in Article 5, paragraph 1, letters a) and b) can submit detailed reports of unlawful conduct in order to protect the entity's integrity. These reports must be based on precise and consistent facts or violations of the entity's organisational and management model of which the reporting party has become aware while performing their duties. The channels through which these reports are submitted guarantee the confidentiality of the reporting party's identity;
- at least one alternative reporting channel that guarantees the confidentiality of the whistleblower's identity via electronic means.
- The prohibition of retaliatory or discriminatory acts, direct or indirect, against the whistleblower for reasons directly or indirectly related to the report.
- In the disciplinary system adopted pursuant to paragraph 2, letter e), sanctions are imposed on those who violate the measures to protect the whistleblower, as well as on those who intentionally or negligently make unfounded reports.

In light of the regulatory changes outlined above and based on the guidance provided in the Confindustria explanatory note of January 2018 and the Assonime circular of 28 June 2018, Model 231 must incorporate a *dedicated Whistleblowing* procedure. This procedure must establish channels specifically for submitting reports based on precise and consistent facts, while ensuring the confidentiality of the whistleblower's identity.
The procedure must also take into account the following measures:

- the identification of a system for managing violation reports that guarantees the anonymity of the *whistleblower*;
- specific training for senior management and their subordinates;
- the integration of the disciplinary system established by Model 231, including sanctions against those who violate the measures to protect the whistleblower, as well as those who intentionally or through gross negligence submit unfounded reports.

Legislative Decree no. 24 came into force on 10 March 2023, with the aim of extending the scope of *whistleblowing* regulations by broadening the subjective and objective scope, as well as the internal channels that companies are required to implement.
In light of the regulatory changes outlined above and the guidance provided in the ANAC Guidelines issued on 12 July 2023, as well as in Confindustria's Operational Guide of October 2023, Model 231 must incorporate a *dedicated Whistleblowing* procedure. This procedure must establish channels specifically for submitting reports based on precise and consistent facts, while ensuring the confidentiality of the whistleblower's identity.
The procedure must also take into account the following measures:

- the identification of a system for managing violation reports that guarantees the confidentiality of the *whistleblower*;
- specific training for senior management and their subordinates;
- the integration of the disciplinary system established by Model 231, including sanctions against those who violate the measures to protect the whistleblower, as well as those who intentionally or through gross negligence submit unfounded reports.

The reporting procedure (*Whistleblowing*) is detailed in the document "Reporting Procedure", which outlines all the methods that can be used for reporting.

6.7. Sensitive activity areas, support processes and the decision-making process

The decision-making process relating to these areas must comply with the following criteria:

- every decision regarding operations within the sensitive activity areas, as identified below, must be recorded in writing;
- there must never be any overlap between the person who decides to carry out a process in a sensitive area and the person who carries out and completes the process;
- there must never be any overlap between those who decide on and implement a process within a sensitive area, and those who have the power to allocate the necessary economic and financial resources.

The main sensitive activities and support processes are indicated below and analysed in detail in the relevant special sections.

Offences against the Public Administration and against the state (special section E):

omissis

Offences relating to the counterfeiting of legal tender, public credit instruments, revenue stamps and identification tools or signs (special section F):

omissis

Corporate offences (special section G):

omissis

Offences against the individual (special section H):

omissis

Offences relating to workplace safety (special section I):

omissis

Offences relating to the receipt, laundering or use of money, goods or benefits of unlawful origin, as well as self-laundering (special section J):

omissis

Offences relating to cybercrime and unlawful data processing (special section K)

omissis

Offences relating to copyright infringement (special section L) *omissis*

Crimes against industry and commerce (special section M)

omissis

Offences pursuant to Article 377-*bis* of the Italian Criminal Code (special section N)

omissis

Offences relating organised crime (special section O)

omissis

Environmental crimes (special section P):

omissis

Offences related to the employment of illegal immigrants (Special Section Q)

omissis

Transnational offences referred to in Italian Law no. 146 of 16 March 2006 (special section R)

omissis

Tax offences (special section S)

omissis

Customs offences (special section T)

macro sensitive activities	support processes
Import and export management	Contract management
Relationships management with the Customs Agency	
Management of the purchase of goods and services	

Offences relating to non-cash means of payment (special section U)

omissis

With regard to:
- offences committed for the purposes of terrorism or subverting the democratic order (art. 25-*quater* of the Decree);
- offences involving female genital mutilation (art. 25-*quater*. 1 of the Decree); - offences relating to market abuse (art. 25-*sexies* of the Decree);
- offences of xenophobia and racism (art. 25 *terdecies*);
- fraud in sports competitions, illegal gambling or betting, and gambling exercised using prohibited devices (art. 25-quaterdecies of the Decree);
- crimes against cultural heritage pursuant to art. 25 septiesdecies of Legislative Decree No. 231/2001 as well as art. 25 duodevicies of the same decree;

as there are no risk areas related to these offences,

it was deemed that the company's activities do not present risk profiles that could result in them being committed in the company's interest or to its advantage.
Therefore, it is considered sufficient to refer to the principles contained in the General Part of the Model and in the Code of Ethics. These principles oblige the recipients of the Model to respect the values of solidarity, morality, respect for the law and fairness.

6.7.1. Archiving documentation relating to sensitive activities and support processes

The activities carried out within the scope of sensitive activities and support processes are adequately formalised, particularly with reference to the documentation prepared during their implementation.

The documentation outlined above, produced and/or available in paper or electronic format, is archived in an orderly and systematic manner by the relevant functions or specifically indicated in detailed procedures or work instructions.

To safeguard company documents and information assets, adequate security measures are implemented to prevent the risk of loss or alteration of documentation relating to sensitive activities and support processes, or unauthorised access to data/documents.

6.7.2. Information systems and computer applications

In order to monitor data integrity and the effectiveness of information systems and/or IT applications used for operational or control activities relating to sensitive activities, processes or related support processes, the following are guaranteed:
- user profiling systems relating to access to modules or environments, and authorisation to access specific areas for each individual user (with the ability to manage authorised data and transactions), on request from those responsible for the Information Systems;
- rules for the correct use of company information systems and aids (hardware and software); - a defined system for Internet browsing (blacklisting, website authorisation etc.);

- implementation of the company email system and creation of a certified email system, with regulated access (for sending and receiving documents);
- a defined and automated password generation and change policy; - automated system access control mechanisms;
- a system for tracking user access (via personal passwords and user IDs) and the operations performed by each user;
- a company-wide monitoring and transaction tracking system that stores data for 6 months;
- automated access blocking or inhibition mechanisms; - mechanisms for disabling user access;
- a defined and automated logging system for recording all transactions conducted on the network;

Identification and differentiated profiling of system administrators;

6.8. Management systems and company procedures

The company has established a framework of formalised procedures to govern its core activities. These procedures are accessible to all employees via the company intranet.
They form an integral part of the management systems that have already been implemented and reported on.
The company is ISO 9001 certified for quality.
The department responsible for drafting, reviewing, and approving each procedure has been clearly identified.
Furthermore, a *process* has been established to authorise the procedures before they can be officially released.

6.9. System of delegations and powers

The authorisation system, which establishes a structured and consistent delegation of functions and powers of attorney throughout the company must comply with the following requirements:

- each delegation must combine a managerial power with the corresponding responsibility and a suitable position in the organisational chart. It must also be updated in the event of organisational changes;
- each delegation must specifically and unambiguously define and describe the managerial powers of the delegate, as well as the individual to whom the delegate reports in the hierarchy;
- the management powers assigned in the delegations and their implementation must align with company objectives;
- the delegate must have spending powers appropriate to the assigned functions;
- the powers of attorney may only be granted to individuals with internal functional delegation or specific assignment, and must include the scope of representation and, where applicable, spending limits;
- only individuals with specific and formal powers may assume obligations towards third parties, in the company's name and on its behalf;
- anyone maintaining relationships with public administrations must be granted a delegation or power of attorney to this effect;
- the Articles of Association set out the requirements and procedures for appointing the manager responsible for preparing accounting and corporate documents.

Dierre's system of delegations and powers, which forms an integral and substantial part of the model and is shown in "Special Section B: Organisational structure and system of delegations".

All powers conferred by delegation or execution correspond exactly to the duties and responsibilities as reported in the company's organisational chart.

6.10. Information and training

6.10.1. Information

To guarantee the effectiveness of the model, Dierre aims to ensure that all recipients have the necessary knowledge,
taking into account their different levels of involvement in sensitive processes.

To this end, Dierre will disseminate the model using the following general methods:
- creating specific, constantly updated web pages on the company intranet. The content of these pages will essentially concern:
1) general information about the Decree and the guidelines adopted for drafting the Model;
2) the structure and main operational provisions of the Model adopted by Dierre;
3) the reporting procedure to the Supervisory Body and the standard form that senior management and employees can use to report any conduct by other employees or third parties that is inconsistent with the contents of the Model.

Once the Model has been adopted, the relevant bodies (e.g. president, general management) will inform all employees that Dierre has adopted an Organisation, Management and Control Model pursuant to the Decree. Further details and information will be provided on the company intranet. A copy of this communication will also be posted on the corporate bulletin board.

New employees will receive information on the adopted Model in their letter of employment, including an information note on the Decree and details of the adopted Model.

6.10.2. Information for external collaborators and partners

All individuals outside the company, including consultants and partners, will be informed that
Dierre has adopted a Model that includes a Code of Ethics. To this end, Dierre will provide these individuals with the website address where the Model and the Code of Ethics can be viewed. They will also be required to formally commit to complying with the provisions contained in these documents.
With regard to external consultants who work closely with Dierre, Dierre will contact them and, through a detailed verification process, ensure that they are familiar with the company's Model and willing to comply with it.

6.10.3. Information for Group Companies

Group companies must be informed of the Model's content and of Dierre's interest in ensuring that its subsidiaries' conduct complies with the provisions of the Decree. They will therefore be informed about the Model when it is adopted.

6.10.4. Training

Training programmes must be evaluated and endorsed by an external consultant who specialises either in corporate administrative liability (Italian Legislative Decree no. 231/2001) or criminal law in general. This consultant will collaborate with the Supervisory Body.

Formal records of the training must be kept.
Training can also be provided *online*, or in hard copy format for employees who cannot access computers.

6.10.5. Training for "senior" personnel

Training for "senior" personnel, including Supervisory Body members, consists of training and refresher courses with mandatory attendance, followed by a final assessment test, which may be oral, to certify the quality of the training received.
Training and refresher courses must be scheduled at the beginning of the year. Training for newly appointed members of the Board of Directors and any new hires in "senior" positions is based on the information included in their employment letters.

Training for "senior" personnel must be divided into two parts: a "general" part and a "specific" part.

The "general" part must contain:
- regulatory, case law and best practice references;
- administrative responsibility of the entity: purpose and rationale of the Decree, the nature of liability and regulatory developments;
- the addressees of the Decree;
- conditions for attributing liability;
- description of the predicate offences;
- types of sanctions applicable to the entity;
- conditions for excluding or limiting liability.

The following activities will also be performed during the training:
- raising awareness of Dierre's commitment to adopting a risk governance and control system;
- describing the structure and contents of the adopted Model and the methodological approach followed for its implementation and updating.

The training regarding the "specific" part focuses on: - providing a detailed description of the different types of offence;
- identifying individuals responsible for offences;
- providing examples of how offences are committed; - analysing the applicable sanctions;
- matching individual offence types with specific risk areas;
- training on the specific prevention protocols developed by the company to avoid the identified risk areas;
- the procedures to be followed regarding communications and training of hierarchical employees, particularly those working in sensitive areas of the company, are described;
- the procedures to be followed with regard to communications, reporting, and collaboration with the Supervisory Body in monitoring and updating the Model are illustrated;
- the managers of company functions that are potentially at risk of crime and their subordinates are informed of the required conduct, the consequences of non-compliance with these procedures and the model adopted by Dierre in general.

6.10.6. Training of other personnel

Training for other personnel begins with an internal briefing note, which will be given to new hires at the time of recruitment.

Training for personnel other than senior management consists of training and refresher courses, with mandatory attendance, followed by a final assessment test, which may be oral—to certify the quality of the training received. Training and refresher courses must be scheduled at the beginning of the year.

Training for personnel other than senior management must be divided into two parts: a “general” part and a “specific” part, which may be optional and/or partial.

The "general" part must contain:

- regulatory, case law and best practice references;
- administrative responsibility of the entity: purpose and rationale of the Decree, the nature of liability and regulatory developments;
- the addressees of the Decree;
- conditions for attributing liability
- description of the predicate offences;
- types of sanctions applicable to the entity;
- conditions for excluding or limiting liability.

The following activities will also be performed during the training:

– raising awareness of Dierre’s commitment to adopting a risk governance and control system;
– describing the structure and contents of the adopted Model and the methodological approach followed for its implementation and updating.

The training regarding the "specific" part focuses on: - providing a detailed description of the different types of offence;

- identifying individuals responsible for offences;
- providing examples of how offences are committed; - analysing the applicable sanctions;
- matching individual offence types with specific risk areas;
- training on the specific prevention protocols developed by the company to avoid the identified risk areas;
- the procedures to be followed regarding communications and training of hierarchical employees, particularly those working in sensitive areas of the company, are described;
- the procedures to be followed with regard to communications, reporting, and collaboration with the Supervisory Body in monitoring and updating the Model are illustrated;
- the managers of company functions that are potentially at risk of crime and their subordinates are informed of the required conduct, the consequences of non-compliance with these procedures and the model adopted by Dierre in general.

Regarding the "specific" training, it should be noted that it will be intended solely for individuals at genuine risk of carrying out activities relating to Legislative Decree no. 231 of 2001, and will be limited to the risk areas with which they may come into contact.

6.10.7. Training for the Supervisory Body

Training for the Supervisory Body is coordinated with the help of an external consultant who specialises in corporate administrative liability (Legislative Decree No. 231/2001) or criminal law in general.

This training aims to provide the Supervisory Body with a high level of technical understanding of the Organisational Model and the company's specific prevention protocols. It also equips them with the necessary tools to carry out their oversight duties adequately.

This mandatory, supervised training can generally be achieved through participation in: 1) conferences or seminars on Legislative Decree No. 231 of 2001; 2) meetings with experts in corporate administrative liability (Legislative Decree No. 231 of 2001) or criminal law. Training and refresher courses are organised for personnel in "senior" positions to improve their understanding of the Organisational Model and the Company's specific prevention protocols.
Training of the Supervisory Body must include the contents of the "general" and "specific" training already described, as well as in-depth information on:

- independence; -
  autonomy;
- continuity of action;
- professionalism;
- relationships with corporate bodies;
- relationships with other bodies responsible for internal control;
- the relationship between the implementation of the Model and other control systems in place within the company;
- *whistleblowing* and the management of reports to protect the confidentiality of whistleblowers;
- reporting on the activities of the Supervisory Body (inspection minutes, meeting reports, etc.);
- sample checklists for inspection activities;
- examples of mapping of sensitive activities and support processes

6.11. Sanctions system

Providing an effective disciplinary system for breaches of the Model's requirements is essential for ensuring the Model's effectiveness.

In this regard, article 6, par. 2 *e*) and art. 7 par. 4 *b*) of the Decree stipulate that the Model should "introduce a suitable disciplinary system to penalise failure to comply with the measures set out in the Model".

Applying the disciplinary penalties set out in the Decree renders criminal proceedings unnecessary, since Dierre has full autonomy in enforcing both the Model and the Code of Ethics, regardless of the nature of offence.

Specifically Dierre's disciplinary system:
- is structured differently according to the recipients, which include individuals in "senior" positions; employees; external collaborators and partners;
- identifies the exact disciplinary sanctions to be adopted against those who commit violations, infringements, evasion or the imperfect or partial application of the requirements contained in the Model. This is all in accordance with the relevant provisions of the NCBA and applicable legislation;

- provides for a specific procedure for applying the aforementioned sanctions and identifies who is responsible for applying them as well as for generally monitoring the enforcement, application and updating of the disciplinary system;
- introduces appropriate means of publication and dissemination;
- includes sanctions against those who violate the measures to protect the person making a report pursuant to the *whistleblowing* procedure, as well as those who, intentionally or through gross negligence submit unfounded reports.

Dierre has drawn up and applied the sanctions system in accordance with the above principles. This system forms an integral and substantial part of the model as “Special Section D”.

6.12. Offences against the Public Administration and against the State

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of articles 24 and 25 of the Decree can be found in "Special Section E: Offences against the Public Administration and against the State”.

6.13. Offences relating to the counterfeiting of legal tender, public credit instruments and revenue stamps

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25 *bis* the Decree can be found in "Special Section F: Offences relating to the counterfeiting of legal tender, public credit instruments, revenue stamps and identification tools or signs”.

6.14. Corporate offences

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*ter* of the Decree can be found in "Special Section G: Corporate offences”.

6.15. Offences against the individual

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*quinquies* of the Decree can be found in "Special Section H: Offences against the individual”.

6.16. Offences relating to workplace safety

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*septies* of the Decree can be found in "Special Section I: Offences relating to safety in the workplace”.

6.17. Offences relating to the receipt, laundering or use of money, goods or benefits of unlawful origin, as well as self-laundering

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*octies* of the Decree can be found in "Special Section J: Offences relating to the receipt, laundering or use of money, goods or benefits of unlawful origin, as well as self-laundering”.

6.18. Offences relating to cybercrime and unlawful data processing

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 24-*bis* of the Decree can be found in "Special Section K: Offences relating to cybercrime and unlawful data processing”.

6.19. Offences relating to copyright infringement

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*novies* of the Decree can be found in "Special Section L: Offences relating to copyright infringement".

6.20. Crimes against industry and commerce

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*bis* 1 of the Decree can be found in "Special Section M: Crimes against industry and commerce".

6.21. Offences pursuant to Article 377-bis of the Italian Criminal Code

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*novies* of the Decree can be found in "Special Section N: Offences pursuant to Article 377-*bis* of the Italian Criminal Code".

6.22. Offences relating to organised crime

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 24-*ter* of the Decree can be found in "Special Section O: Offences relating to organised crime".

6.23. Environmental crimes

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*undecies* of the Decree can be found in "Special Section P: Environmental crimes".

6.24. Offences related to the employment of illegal immigrants

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 25-*duodecies* can be found in "Special Section Q: Offences related to the employment of illegal immigrants".

6.25. Transnational offences referred to in Italian Law no. 146 of 16 March 2006

A detailed description of the analysis activities performed and the protocols adopted by Dierre according to the provisions of art. 10 of Law 146 of 16 March 2006 of the Decree can be found in "Special Section R: Transnational offences referred to in Italian Law no. 146 of 16 March 2006".

6.26. Tax offences

A detailed description of the analysis activities performed and the protocols adopted by the company according to the provisions of art. 25-*quiniquiesdecies* of the Decree can be found in "Special Section S: Tax offences".

6.27. Offences relating to smuggling

A detailed description of the analysis activities performed and the protocols adopted by DIERRE regarding the provisions of art. 25-*sexiesdecies* of the Decree can be found in "Special Section T Offences relating to smuggling".

6.28. Offences relating to non-cash means of payment

A detailed description of the analysis activities performed and the protocols adopted by DIERRE according to the provisions of art. 25-*octies.1* of the Decree can be found in "Special Section U: Offences relating to non-cash means of payment".

6.29. Financial resource management

Art. 6, par. 2 c) of the Decree requires the company to establish specific procedures for managing financial resources to prevent offences being committed.

To this end, Sintesi has adopted some key principles to be followed in the management of financial resources within its own procedures:

- all transactions relating to financial management must be carried out via the company's current accounts;
- checks on balances and cash transactions must be carried out periodically;
- the treasury management department must define and maintain a specific formalised procedure for opening, using, controlling and closing current accounts in accordance with the company's credit policy and based on adequate segregation of duties and compliance with accounting standards;
- senior management must define the medium- and long-term financial requirements and the sources and forms of funding, providing evidence of this in specific reports.
- Regarding the payment of invoices and expenditure commitments, the company requires that:
- the invoice is checked in all respects (correspondence, calculations, taxation, receipt of goods or services); - the invoice is recorded independently of the accounting records and no payment is made without specific authorisation from the Administration and Finance Office Manager and the person who placed the order;
- all borrowings for financing purposes, including derivative contracts for hedging and speculation, must be approved by the Board of Directors.

6.30. Supervisory body

In compliance with the provisions of Article 6, paragraph 1, letter b, of the Decree, which stipulates that responsibility for monitoring the operation of the Model and ensuring its updating shall be entrusted to a Company body with its own powers of initiative and control, known as the Supervisory Body, the Company has identified and appointed this Body. For details, please refer to "Special Section C: Structure, composition, regulations and functioning of the Supervisory Body".

6.31. Adoption of the model and the supervisory body within the corporate group

Any companies that are directly or indirectly controlled by Dierre, or that belong to the same group (hereinafter referred to as "the Group"), must establish their own "Organisation and Management Model", in accordance with the specifications set out in the Decree.

When doing so, Group Companies can use the model adopted by Dierre as a reference, adapting it to their individual businesses, especially the specific sensitive areas/activities identified within them.
Each group company must set up its own Supervisory Body.

The Supervisory Body of each Group Company:

- may, in the performance of its functions, make use of the resources allocated to Dierre's Supervisory Body, on the basis of a pre-established contractual relationship with Dierre and in accordance with the confidentiality obligation;
- will have to coordinate with Dierre's Supervisory Body to ensure the adoption and implementation of a model that can prevent offences under *Italian* Legislative Decree no. 231 of 2001;
- must promptly notify Dierre's Supervisory Body of any breaches committed by company directors;
- must communicate the adopted Model and any updates;

- must report, at least annually, to Dierre's Supervisory Body.

6.32. Procedure for appointing the entity's defence counsel in cases where the legal representative is deemed incompatible

In ruling no. 38149, issued on 10 October 2022, the Supreme Court of Cassation clarified that a legal representative who is under investigation or has been accused of the predicate crime is prohibited from appointing legal counsel for the company in cases of corporate criminal liability. This prohibition is set out in Article 39 of Legislative Decree no. 231 of 2001.

The *rationale* behind this prohibition is to prevent the entity's right to defence being restricted when the individual is both under investigation and representing the entity in court. Otherwise, the entity might be forced to adopt conflicting defence strategies at the highest level.

In line with the Supreme Court of Cassation's case law, the company established an adequate chain of powers of representation to prevent its legal counsel from being appointed in proceedings that conflict with the representative's interests with regard to the predicate offence.

Specifically, if the President/CEO is unable to appoint counsel due to incompatibility, they may appoint one of the following:

(i) another managing director

(ii) a special attorney specifically identified by the board of directors;

(iii) if all of the aforementioned individuals are incompatible, the board of directors, convened on an urgent basis, may delegate the appointment to a specific director.