Approved by BoD on 19/03/2009
Amended by BoD of 28/09/2023

Unipol Gruppo S.p.A.

Organization, Management and Control Model

(pursuant to Italian Legislative Decree 231/2001)

Disclaimer English Translation

Note that this document represents an English translation of the original version "Modello di Organizzazione, Gestione e Controllo," originally issued in Italian.

The accuracy and conceptual consistency of the English version of this document may not be ensured. In case of any discrepancies or doubts in the interpretation of the document, official reference must be made to the Italian-language version.

Index

General Section

GENERAL SECTION

1 INTRODUCTION

1.1 DEFINITIONS

Addressees	Executives and employees under their management or supervision, including business partners and suppliers
Collaborator	Independent contractors who maintain business relationships with the institution in various capacities (consultants, professionals, etc.).
Consob	Commissione Nazionale per le Società e la Borsa (The Italian Companies and Stock Exchange Commission).
Confindustria Guidelines	Guidelines for the conception of organization, management, and control models pursuant to Legislative Decree 231/2001 issued by Confindustria pursuant to art. 6 paragraph 3 of the Legislative Decree 231/01.
Decree or Legislative Decree 231/2001	Legislative Decree No.231 dated 8th June 2001 "Rules on the administrative liability of legal entities, companies and associations with or without legal personality" and subsequent amendments.
D. Lgs. 231/2007	Legislative Decree dated 21st November 2007, n. 231, as amended by Decree. n. 90/2017, regarding Anti-money laundering dispositions aimed at protecting the financial system from criminal or terrorist money laundering.
Employees	Employees on the Company's payroll, as well as staff in the Company's workforce and seconded including personnel operating there with a temporary employment contract.
Entities	Legal entities, companies and associations including those without a legal personality.
Executives	Individuals who perform functions of representation, administration, or management of the company or of one of its organizational units with financial and functional autonomy, as well as persons who exercise, even de facto, the management and control thereof
Individuals under the management or supervision of the executives	Persons under the management or supervision of Executives
ISVAP	Institute for the Supervision of Private Insurance and Collective Interest
IVASS	The Italian Institute for the Supervision of Insurance, established by Law No 135 og 7 August 2012 which, from 1 January 2013, took over all powers, functions, and competences of ISVAP

Model or OMM	This model of organization, management, and control, as provided for in Article 6, paragraph 1(a), of Legislative Decree 231/2001.
Offences	The offenses (crimes and violations) referred to in Art. 24 et seq. of Legislative Decree 231/2001 as amended.
SB or Supervisory Body	Body described in art. 6, paragraph 1, letter b) of Legislative Decree 231/2001, assigned responsibility for supervising the functioning of and compliance with the Model and ensuring it is up-to-date.
T.U.F.	Italian Legislative Decree No. 58 of 24 February 1998, "The Consolidated Law on financial intermediation
U.I.F.	Financial Intelligence Unit set up at the Bank of Italy
Unipol Group (also UG, Unipol, Company or Parent Company)	Unipol Gruppo S.p.A.
UnipolSai	UnipolSai Assicurazioni S.p.A.

1.2 Legislative Decree 231/2001

Italian Legislative Decree 231/2001, was issued in compliance with art. 11 of Law no. 300/2000 in order to align the Italian legislation on corporate liability to certain international conventions adopted by Italy , such as the Brussels Convention of 26 July 1995 on the protection of the European Communities' financial interests, the Convention of 26 May 1997, also signed in Brussels, on the fight against corruption involving officials of the European Community and the Member States and the OECD Convention of 17 December 1997 on combating bribery of foreign public officials in international business transactions. The Decree 231/2001 introduced into the Italian legal system " administrative liability on the part of legal entities and companies, associations or bodies which are not corporations" for specific types of offenses (referred to as "predicate offenses") committed by their executives and employees.

Legislative Decree 231/2001 can therefore be understood as a "system rule" that over the years has been implemented with the provision of new types of predicate crimes, subsequently listed in detail (Annex 2).

The legislation in question is the result of a legislative technique which, borrowing the principles of the criminal offence and the administrative offense, has introduced into the Italian legal system a punitive system against company that is added to and integrated with the pre-existing penalty systems.

A criminal court has jurisdiction to rule with respect to administrative offences and is competent to rule on the administrative liability of the Entity and to apply, in case of conviction, the established sanctions and/or penalties.

Regarding market abuse, it should be noted that, according to the provisions of art. 187 – quinquies of the T.U.F., the administrative liability of the entity is also established when the conduct of individuals working for the entity can be qualified as an administrative offense. In this context, the related sanctions are applied by Consob. Also in terms of tax offences, the liability of the entity pursuant to Legislative Decree 231/2001 is added to that envisaged in Legislative Decree 471/1997, which entails the application of administrative penalties.

The Entity may be held liable if one of the offences specifically set forth in Legislative Decree 231/2001 is committed in its interest or for its benefit:

a) by an individual who performs representation, administration or management of the Entity ("top executives") or of one of its organizational units with financial and functional autonomy, as well as by an individual who exercises, even de facto, the management and control thereof;
b) by individuals under the management or supervision of one of the entity's executives.

If a top executive commits an administrative offence, the law presumes the Entity to be liable, in consideration of the fact that these persons express, represent and implement the management policy of the same (Article 5, paragraph 1, letter a) of Legislative Decree 231/2001).

When a person subject to the direction or supervision of others commits an offence, the liability of the Entity is configurable only if the offence has been made possible by its failure to comply with the obligations of direction and supervision (Article 5, paragraph 1, letter b) of Legislative Decree 231/2001): such non-compliance must be demonstrated by the Public Prosecutor.

The liability of the Entity is however excluded in the event that the perpetrator(s) of the offence acted in their own interest or that of third parties.

The Entity is also liable if the perpetrator of the offence has not been identified or cannot be charged and in the event that the offence is extinguished for a cause other than amnesty (art. 8 paragraph 1, letter. a) and b) of Legislative Decree 231/2001).

In the event of an offence committed abroad, the entities that have their headquarters in the territory of the Italian State are in any case prosecuted, provided that the State of the place where the offence-act was committed does not proceed against them (Article 4, paragraph 1, of Legislative Decree 231/2001).

At present, the administrative liability of the Entities may derive from the commission of specific types of offences provided for by the Decree, which are listed below:

- Undue receipt of funds, fraud to the detriment of the State or a public body or the European Union or for the achievement of public funds and IT fraud to the detriment of theState or a public body and procurement fraud: **art. 24**[1]
- Computer crimes: **art. *24-bis***
- Crimes of organized crime: **art. *24-ter***
- Embezzlement, extorsions, bribery to give or promise benefits, corruption, and abuse of office: **art. 25**[2]
- Counterfeit of currency, public credit cards, revenue stamps and identifying instruments or signs: **art. *25-bis***
- Crimes against industry and trade: **art. *25-bis.1***
- Corporate offences: **art. *25-ter***
- Offences with the purpose of terrorism or subversion of the democratic order: **art. *25-quarter***
- Practices of mutilation of female genital organs: **art. *25-quarter.1***
- Crimes against the individual personality: **art. *25-d***
- Illicit intermediation and labour exploitation: ***art. 25 quinquies, paragraph 1, letter a)***
- Market abuse: **art. *25-sexies***
- Offences of manslaughter or actual or grievous bodily harm related to violation of the occupational health and safety standard: **art. *25-septies***
- Receiving stolen goods, money laundering and use of money, goods, or benefits of illicit origin, as well as self-laundering: **art. *25-octies***[3]
- Fraud and falsification of means of payment other than cash: **art. 25-octies 1**[4]
- Infringement of copyright: **art. *25-novies***
- Incitement to not make statements or make false statements to the judicial authority: **art. *25-decies***
- Environmental offences: **art. *25-undecies***
- Employment of illegally staying third-country nationals: **art. *25-duodecies***[5]
- Racism and Xenophobia: ***art. 25-terdecies***[6]
- Fraud in sports competitions, abusive gambling or betting and gambling by means of prohibited devices: **art. *25-quaterdecies***[7]
- Tax offences: **art. *25-quinquiesdecies***[8]
- Smuggling offences: **art. *25-sexiesdecies***[9]
- Offences against cultural heritage: **art. *25-septiesdecies***[10]
- Recycling of cultural property and devastation and looting of cultural and landscapeproperty: **art. 25- duodevicies**[11]

[1] Article amended by Legislative Decree 75/2020
[2] Article amended by Legislative Decree 75/2020
[3] Legislative Decree 195/2021 has indirect implications on Article 25-g, although not amending it, as it makes amendments to the articles of the Criminal Code referred to in Article *25-gties* itself. These changes have been considered in the relevant Special Part.
[4] Article introduced by Legislative Decree 184/2021
[5] Article amended by Law no. 161 of 2017, which extended the liability of the Body to the crimes provided for in paragraphs 3, *3-bis, 3-ter* and 5 of art. 12 of Legislative Decree 286/1998 (T.U. Immigration)
[6] Article amended by Legislative Decree 21/2018: the crime referred to (pursuant to Article 3, paragraph 3-bis, Law no. 654 of 13 October 1975) has been moved to the Criminal Code (Article 604-bis).
[7] Article introduced by Law 39/2019
[8] Article introduced by Law 157/2019 and amended by Legislative Decree 75/2020
[9] Article introduced by Legislative Decree 75/2020
[10] Article introduced by Law no. 22 of 2022
[11] Article introduced by Law no. 22 of 2022

Liability of the Entity may also be established in relation to the cross-border offences referred to in Article 10 of Law no. 146/2006 "Ratification and execution of the United Nations Convention and Protocols against Transnational Organized Crime, adopted by the UN General Assembly on 15 November 2000 and 31 May 2001 " (organized crimes, obstruction of justice, aiding illegal immigration).

If one of the offences specifically indicated is committed, the “administrative” liability of the entity is added to the criminal liability of the natural person who committed the offence, if and insofar as all other regularity requirements are met.

Further details on the offences provided for by Legislative Decree 231/2001 can be read in Annex 4.

For the purposes of preparing this Organization, Management and Control Model, all the types of crime present in the Decree have been taken into consideration and the following types of crime have been considered abstractly conceivable (for the purposes of this section *Italian Criminal Code* will be referred to as “cod. pen.” and *Italian Civil Code* as “cod. civ.”) :

Crimes in relations with the Public Administration (articles 24 and 25 of the Decree)

- Embezzlement (art. 314, paragraph 1, cod. pen.);
- Embezzlement by profiting from the error of others (art. 316, cod. pen.);
- Embezzlement to the detriment of the State (art. 316-bis, cod. pen.);
- Undue receipt of funds to the detriment of the State (art. 316-ter, cod. pen.);
- Corruption or bribery in the exercise of the office (art. 318, cod. pen.);
- Corruption or bribery for an act contrary to the duties of office (art. 319, cod. pen.);
- Corruption in judicial proceedings (art. 319-ter, cod. pen.);
- Bribery to give or promise benefits (article 319-quarter of the cod. pen.);
- Bribery of a person in charge of a public service (art. 320, cod. pen.);
- Incitement to corruption (art. 322, cod. pen.);
- Embezzlement, extortion, bribery to give or promise benefits, corruption and incitement to corruption, abuse of office of members of the ICC or of the bodies of the EC of officials of the EC or foreign states (article 322-bis of the cod. pen.);
- Abuse of office (art. 323, cod. pen.);
- Trafficking in illicit influences (Article 346-bis, cod. pen.);
- Fraud to the detriment of the State, another public body or the European Union (art. 640, paragraph 2, n. 1 cod. pen.);
- Aggravated fraud to obtain public funds (art. 640-bis, cod. pen.);
- Computer fraud (art. 640-ter, cod. pen.).

For a brief description of the types of offences against the Public Administration and examples of related conduct, please refer to **Special Part 1** "Offences against the Public Administration".

Corporate offences (art. 25-ter of the Decree)

- False corporate disclosure (art. 2621, cod. civ.);
- False corporate disclosure of listed companies (art. 2622, of the cod. civ.);
- Obstruction of control (art. 2625, cod. civ.);
- Unlawful restitution of contributions (article 2626, of the cod. civ.;
- Unlawful distribution of profits and reserves (art. 2627, cod. civ.);
- Unlawful transactions involving shares or shareholdings (article 2628, of the cod. civ.);
- Transactions to the detriment of creditors (article 2629, cod. civ.);
- Failure to disclose conflict of interest (art. 2629-bis of the cod. civ.);
- Fictitious formation of share capital (article 2632, of the cod. civ.);
- Corruption between private parties (article 2635 of the cod. civ.);
- Attempted bribery between private parties (2635 bis, cod. civ.);

- Unlawful influence over the shareholders' meeting (art. 2636, of the cod. civ.);
- Obstruction of the supervisory functions of the public authorities (art. 2638, cod. civ.);
- False or omitted declarations for the issuance of the preliminary certificate (article 54, Legislative Decree 19/2023).

For a brief description of the types of corporate offences and examples of related conduct, please refer to **Special Part 2** "Corporate Offences".

Crimes and administrative offences of insider dealing, market manipulation and rigging (articles 25-sexies and 25-ter of the Decree)

- Abuse or unlawful disclosure of inside information. Recommendation or inducement of others to the commission of insider dealing pursuant to article 184;
- Abuse and unlawful disclosure of inside information pursuant to art. 187-bis T.U.F.;
- Market manipulation referred to in articles 185 and 187-ter T.U.F;
- Rigging pursuant to art. 2637 cod. civ.

For a brief description of cases concerning crimes and administrative offenses of insider dealing, market manipulation and rigging and examples of related conduct related conduct, please refer to **Special Part 3** "Crimes and administrative offenses of insider dealing, market manipulation and rigging ".

Crimes of receiving stolen goods, money laundering, self-laundering and crimes with the purpose of terrorism or subversion of the democratic order (articles 25-octies and 25-quarter of the Decree

- Receiving stolen goods (art. 648, cod. pen.);
- Money Laundering (art. 648-bis cod. pen.);
- Use of money, goods or benefits of illicit origin (art. 648-ter, cod. pen.);
- Self-laundering (art, 648 ter 1, cod. pen.);
- Criminal Associations with the purpose of terrorism, including international terrorism, or subversion of the democratic order (art. 270-bis, cod. pen.);
- Aiding and abetting criminal organization members (art. 270-ter, cod. pen.);
- Financing of conduct for terrorist purposes (art. 270-quinquies.1 cod. pen.);
- Misappropriation of assets or money subject to seizure (art. 270-quinquies.2 cod. pen.);
- Acts of nuclear terrorism (art. 280-ter cod. pen.);
- Art. 2 - International Convention for the Suppression of the Financing of Terrorism. New York 9 December 1999.

For a brief description of cases concerning offences of receiving stolen goods and money laundering, and offences with the purpose of terrorism or subversion of the democratic order and examples of related conduct, please refer to **Special Part 4** "Crimes of receiving stolen goods, money laundering, self-laundering and crimes with terrorist purposes or subversion of the democratic order".

Computer crimes (art. 24-bis of the Decree)

- Digital documents (art. 491-bis cod. pen.);
- Unauthorized access to a computer or telematic system (art. 615-ter cod. pen.);
- Illegal possession, dissemination and abusive installation of equipment, codes and other means suitable for access to computer or telematic systems (art. 615-quarter of the cod. pen.);
- Illegal possession, dissemination or abusive installation of equipment, devices, or programs aimed at damaging or interrupting an IT or telematic system (art. 615-quinquies cod. pen.);
- Illegal interception, obstruction or unlawful interruption of IT or telematic communications (art. 617-quarter cod. pen.);

- Installation of equipment to intercept, prevent or interrupt computer or telematic communications (art. 617-quinquies cod. pen.);
- Damage to information, data and computer programs (art. 635-bis cod. pen.);
- Damage to information, data and computer programs used by the State or other public body or otherwise of public interest (art. 635-ter cod. pen.);
- Damage to computer or telematic systems (art. 635-quarter cod. pen.);
- Computer fraud by the entity providing digital signature certification services (art. 640-quinquies, cod. pen.).

For a brief description of cases concerning computer crimes and examples of related conduct, please refer to **Special Part 5** " Computer crimes".

Manslaughter or serious or very serious injuries committed with violation of the occupational health and safety standards (art. 25-septies of the Decree)

- Manslaughter (art. 589 cod. pen.);
- Culpable personal injury (art. 590, cod. pen.);

For a brief description of the types of offences for manslaughter and injuries related to violation of occupational health and safety standards at work and examples of related conduct, please refer to **Special Part 6** " Manslaughter or serious or very serious injuries committed with violation of the occupational health and safety standards ".

Organized crime and cross-border offences (art. 24-ter of the Decree and Law 16 March 2006, 146)

- Criminal conspiracy (art. 416 cod. pen.);
- Mafia-type associations, including foreign ones, (art. 416-bis cod. pen.);
- Provisions against illegal immigration (Article 12, paragraphs 3, 3-bis, 3-ter and 5, Legislative Decree 286/1998– T.U. Immigration).

For a brief description of cases concerning organized crime and cross-border crimes and examples of related conduct, please refer to **Special Part 7** "Organized crime and cross- crimes".

Environmental offences (art. 25-undecies of the Decree)

- Unauthorized waste management activities (Article 256 of Legislative Decree 152/2006);
- Violation of the obligations of disclosure, keeping of mandatory registers and forms (Article 258, paragraph 4, second sentence, Legislative Decree 152/2006);
- Illegal traffic of waste (Article 259, paragraph 1, Legislative Decree 152/2006).
- Environmental pollution (art. 452 bis cod. pen);
- Environmental disaster (art. 452 quarter, pen. code);
- Environmental offences without criminal intent (art. 452 quinquies, cod. pen.).

For a brief description of cases concerning environmental crimes, and examples of he related conduct, please refer to **Special Part 8** "Environmental offences ".

Copyright infringement (art. 25-novies of the Decree)

- Protection of copyright and other rights related to its exercise (articles 171, 171-bis, 171-ter, 171-septies and 171-octies L. 633/ 1941).

For a brief description of cases concerning copyright infringement offences and examples of related conduct, please refer to **Special Part 9** "Copyright infringement".

Employment of illegally staying third-country nationals (Article 25-duodecies of the Decree)

- Fixed-term and open-ended employment (Article 22, paragraph 12-bis, Legislative Decree 286/98).

For a brief description of cases concerning the crime of employment of third-country nationals whose residence permit is irregular and examples of related conduct, please refer to the **Special Part 10** "Employment of illegally staying third-country nationals".

Incitement to not make statements or make false statements to the judicial authority (art. 25-decies of the Decree)

- Incitement to not make statements or make false statements to the judicial authority (art. 377-bis cod. pen.)

For a brief description of cases concerning the crime of Incitement to not make statements or make false statements to the judicial authority and examples of related conduct, please refer to **Special Part 11** " Incitement to not make statements or make false statements to the judicial authority".

Illicit brokering and labor exploitation (art. 25-quinquies of the Decree)

- Illicit brokering and labor exploitation (art. 603-bis, cod. pen.)

For a brief description of cases concerning the crime of illicit brokering and labor exploitation and examples of related conduct, please refer to **Special Part 12** "Illicit brokering and labor exploitation".

Fraud in sports competitions (art. 25-quaterdecies of the Decree)

- Fraud in sports competitions (art. 1, Law 13 December 1989, n. 401).

For a brief description of cases concerning fraud in sports competitions and examples of related conduct, please refer to **Special Part 13** "Fraud in sports competitions".

Tax offences (art. 25-quinquiesdecies of the Decree)

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (Article 2, Legislative Decree 74/2000);
- Fraudulent declaration through other artifices (Article 3, Legislative Decree 74/2000);
- Inaccurate declaration (Article 4, Legislative Decree 74/2000);
- Omitted declaration (Article 5, Legislative Decree 74/2020);
- Issuance of invoices or other documents for non-existent transactions (Article 8, Legislative Decree 74/2000);
- Concealment or destruction of accounting documents (Article 10, Legislative Decree 74/2000);
- Undue compensation (Article 10-quarter, Legislative Decree 74/2000);
- Fraudulent tax evasion (Article 11, Legislative Decree 74/2000).

For a brief description of cases concerning tax crimes and examples of related conduct, please refer to **Special Part 14** "Tax crimes".

1.3 Penalities against the entity

The penalties provided for administrative offenses dependent on crime are:

a. Fines;
b. Disqualification sanctions;
c. Confiscation;
d. Publication of the conviction.

(a) Fines

Pecuniary administrative sanctions, governed by articles 10 and following of Legislative Decree. 231/2001, constitute the "basic" sanction of necessary application, for the payment of which the Entity is liable with its assets or with the common fund.

The Legislator has adopted an innovative criterion for measuring this sanction, attributing to the Judge the obligation to proceed with two different and subsequent appreciation assessments, in order to better adapt the sanction to the seriousness of the fact and to the economic conditions of the Entity.

The determination of the financial penalties that may be imposed pursuant to Legislative Decree 231/2001 is based on a system of units. For each offense, in fact, the law in the abstract determines a minimum and maximum number of units, on the model of the legal frameworks that traditionally characterize the sanctioning system.

With the first evaluation, the Judge determines the number of units (not less than one hundred, nor more than one thousand, without prejudice to the provisions of art. 25-septies "Manslaughter or serious or very serious culpable injuries, committed with violation of the rules on the occupational health and safety standards" which in the first paragraph in relation to the crime referred to in Article 589 of the Criminal Code. committed with violation of art. 55, paragraph 2, Legislative Decree 81/2008 provides for a penalty equal to one thousand units), considering:

- the seriousness of the act;
- the degree of liability of the Entity;
- the activity carried out to eliminate or mitigate the consequences of the act and to prevent the commission of further offenses.

During the second assessment, the Judge determines, within the minimum and maximum values predetermined in relation to the offenses sanctioned, the value of each unit (from a minimum of Euro 258 to a maximum of Euro 1,549) "on the basis of the economic and financial conditions of the entity in order to ensure the effectiveness of the penalty" (Article 11, paragraph 2, D. Lgs. 231/2001).

Article 12 of Legislative Decree Regulation (EC) No 231/2001 establishes for a series of cases in which the financial penalty is reduced. They are summarised in the table below, indicating the reduction made and the conditions for the application of the reduction.

1/2 (and cannot exceed euro 103,291.38)	• the perpetrator committed the offence in his/her own interest or in the interest of third parties and the Entity did not benefit or gained benefit from it. • the financial damage caused is negligible.
from 1/3 to 1/2	[Before the opening statement of the first instance hearing] • The entity has fully compensated the damage and has eliminated the harmful or dangerous. • consequences of the crime or has in any case effectively worked in this regard; or • An organizational model has been implemented and made operational to prevent crimes of the kind that occurred.
from 1/2 to 2/3	[Before the opening statement of the first instance hearing] • The Entity has fully compensated the damage and has eliminated the harmful or dangerous consequences of the crime or has in any case effectively worked in this regard; and • An organizational model has been implemented and made operational to prevent crimes of the kind that occurred.

(b) Disqualification sanctions

Disqualification sanctions provided for by Legislative Decree 231/2001 are:

1. disqualification from exercising the business activity;
2. prohibition on entering into contracts with the public administration, unless done so in order to obtain a public service;
3. suspension or cancellation of authorizations, licenses or concessions serving to commit the unlawful act;
4. exclusion from benefits, loans, contributions or subsidies and possible cancellation of those already granted;
5. prohibition on publicizing goods or services.

Unlike the fine, which cannot be modified, disqualification sanctions apply only in relation to the offences for which they are expressly established and when at least one of the conditions referred to in art. 13, D. Lgs. 231/2001, indicated below is met:

- *"the entity has derived a significant profit from the offence and the offence has been committed by top executives or by persons under the management of others and, in this case, the commission of the offence has been determined or facilitated by serious organizational shortcomings";*
- *"in the event of repetition of offences" (Article 20 specifies that there is repetition "when the entity already convicted definitively at least once for an offence dependent on a crime, commits another within five years following the final sentence ").*

In any case, bans are not applied when the crime was committed in the predominant interest of the author or third parties and the Entity has gained a minimum or no advantage, or the financial damage caused is particularly minor. The application of disqualification sanctions is also excluded if the Entity has carried out the remedial conduct provided for by art. 17, D.Lgs. 231/2001 and, more precisely, when the following conditions are met:

- "*the entity has compensated in full for the damage and has eliminated the harmful or dangerous consequences of the crime or has otherwise made effective efforts to do so";*

- *"the entity has eliminated the organizational shortcomings that led to the crime through the adoption and implementation of organizational models suitable for preventing crimes of the kind that occurred";*
- *"the entity has made available the profit obtained for the purpose of confiscation".*

Disqualification sanctions can last between three months to two years and the choice of the measure to be applied as well as its duration is made by the Judge on the basis of the same criteria previously indicated for the measurement of the financial penalty, " taking into account the suitability of the individual penalties to prevent offenses of the type committed" (art. 14, D. Lgs.. 231/2001). Article 25 paragraph 5 of Legislative Decree no. Legislative Decree 231/2001 provides for a significant exception, regarding certain crimes of corruption, for which a significant increase in the duration of bans is ordered:

- if the offence is committed by top management, the duration of the ban is between 4 and 7 years;
- if the offence is committed by a person "under management" the duration of the ban is between 2 and 4 years.

The prohibition of the activity has a residual nature compared to the other disqualification sanctions.

The ban on exercising its business activity and the suspension or revocation of authorizations, licenses or concessions functional to the commission of the offense cannot be applied as a precautionary measure, just as the commissioner pursuant to art. 15 of the Decree, to SIM, SGR, SICAV and SICAF (art. 60-bis, paragraph 4, T.U.F.), to Banks (art. 97-bis, paragraph 4, D.L.gs. 1 September 1993, n. 385, T.U. Bancario) and to Insurance and Reinsurance companies (pursuant to Article 266, paragraph 4, Legislative Decree no. 209 of 7 September 2005, Private Insurance Code).

It should also be noted that the Public Prosecutor reports the registration of the entities in the crime publication register to Consob, Bank of Italy and IVASS, as the latter are the only parties responsible for the execution of the aforementioned bans.

(c) Confiscation

Pursuant to art. 19, D.Lgs. 231/2001 confiscation of the price or profit gained from the offence is always arranged, together with the conviction sentence, or its economic equivalent, except for the part that can be returned to the injured party and without prejudice to the rights acquired by third parties in good faith. For all intents and purposes, "price" means the money or other economic benefits given or promised to induce another subject to commit a crime, and "profit" means immediate economic utility obtained.

As evidenced by case law (Court of Cass., VI sec. pen. Sent. N. 34505 of 2012), to order the preventive confiscation, the Judge must assess the actual validity of the charge and identify serious evidence of responsibility of the Entity.

(d) Publication of the conviction

The publication in one or more newspapers of the conviction sentence in part or in full may be ordered by the Judge, together with its posting in the municipality where the Entity has its office, when a ban is imposed. The decision is published, by the clerk of court's office, and costs are paid by the Entity.

1.4 Exemption from liability

Legislative Decree 231/2001 establishes that the Entity is not liable for the offences indicated above if:

- top executives and persons under their management have acted in their own interest or in the interests of third parties;
- top executives acted fraudulently evading the Model;
- the company proves that it has adopted and effectively implemented "organization, management and control models" suitable for preventing criminal offenses of the type that occurred (Article 6, Legislative Decree 231/2001).

The adoption of a Model specifically calibrated for the risks to which the Entity is exposed, aimed at preventing specific offenses through the establishment of rules of conduct, is a preventive measure and is the first layer of control to the risk control system. The Entity will not, therefore, be subject to penalty where it proves to have adopted and implemented organizational, managerial and control measures aimed at avoiding offences and, in any case, such that they are:

- suitable, i.e., to ensure the performance of activities in compliance with the law, as well as to promptly identify and eliminate risk situations;
- effective, i.e., proportionate to the need to ensure compliance with the law and, therefore, subject to periodic review to make any changes that may be necessary in the event of significant violations of the requirements, or in the event of changes in organization or activity. Among other things, provision must be made for a disciplinary system capable of sanctioning non-compliance with organizational measures.

The Law also provides that the Models may be adopted based on codes of conduct drawn up by trade associations ("Guidelines"), communicated to the Ministry of Justice which, in agreement with the competent Ministries, may formulate observations within 30 days on the suitability of the models to prevent offences.

2 REFERENCE USED IN PREPARING THE MODEL

The drafting of this Model has considered, among other things, reference best practice, with particular regard to the Confindustria Guidelines, the ANIA Guidelines and the recommendations of criminal case law.

2.1 Confindustria Guidelines

Confindustria Guidelines outline the fundamental activities that each entity must carry out, preparatory to the implementation of its Model, represented by:

- the identification of potential risks: i.e., the analysis of the business context to identify in which areas or sectors of activity and according to which methods events detrimental to the objectives indicated by the Decree could occur abstractly;
- the design of the control system (so called "Protocols" for training, planning and implementation of the institution's decisions), i.e., the assessment of the existing system within the institution for the prevention of crime and its possible adaptation, in terms of its ability to effectively counteract the identified risks.

The components of the control system must be guided by the following principles:

- verifiability, documentability, coherence and consistency of each operation ("*every operation, transaction, action must be verifiable, documented, consistent and congruous*");
- application of the principle of segregation of duties ("*no one can manage an entire process independently*");
- documentability of controls ("*controls must be documented*");
- adequate sanctioning system for the violation of the rules of the Code of Ethics and the Models;
- identification of the requirements of the SB, as represented in paragraph 5 below.
- provision of methods for managing financial resources;
- reporting obligations towards the SB;
- existence of an internal system for reporting violations (so-called "whistleblowing" reporting).

It is understood that the Models adopted must be proportionate in size and commensurate to the risks faced by the Entity, and to this end may also deviate from the Guidelines which are broader by nature.

2.2 ANIA Guidelines

ANIA highlights that, Models that are truly suitable for preventing the offences considered in Legislative Decree 231/2001, carefully follow the principles identified by their Guidelines, which provide that the Entity must have:

- established standards and adopted control procedures, reasonably designed to reduce the possibility of illegal conduct within the corporate structure.
- assigned responsibility for overseeing compliance with the formalized standards and procedures adopted by the company;
- taken concrete steps to effectively communicate standards and procedures to employees, agents, corporate bodies, external consultants and suppliers;
- taken reasonable steps to achieve effective adherence to standards, using monitoring and auditing

systems reasonably suited to uncovering any illegal conduct, introducing, to this end, a reporting system that allows employees, corporate bodies, external consultants and suppliers to report cases of violation of rules, without fear of retaliation;

- implemented the standards, through appropriate disciplinary mechanisms, providing for the imposition of penalties against those responsible;
- taken all steps reasonably necessary, making changes to the OMM where appropriate, to give an appropriate response to the violation and to prevent similar violations from occurring in the future.

To allow the conception of Models that are sufficiently flexible, ANIA suggests paying further attention to the changes and evolutions that have occurred within the corporate structures and outlines the functional characteristics of the Model.

2.3 IVASS Regulation n. 38 /2018 (Corporate governance system)

This Model is part of the broader Group corporate governance system, which - through an effective internal control and risk management system - allows the sound and prudent management of the Group, while considering the interests of the companies that are part of it and the ways in which these interests contribute to the Group's common objective in the long term, also in terms of safeguarding corporate assets.

IVASS Regulation no. 38 of 3 July 2018 (the "Regulation 38/2018") and for what concerns here:

- highlights the need for the control functions and bodies of the Parent Company (Board of Statutory Auditors, Supervisory Body, fundamental functions[12], etc.) to work together with adequate information flows and for liaison mechanisms to be defined with the bodies and functions of the other Group companies;
- requires adoption of a Group code of conduct that promotes operational fairness and respect for integrity and ethical values by all personnel, as well as prevents deviant conduct;
- emphasizes the correct structuring of corporate IT systems and cyber security.

The contents of Regulation 38/2018 complement the crime prevention system represented by this Model.

[12] *Audit, Risk management, Compliance, Actuary functions*

3 ADOPTION OF THE MODEL

3.1 The Role and activities of Unipol Group

Unipol is an issuer with shares listed on the Italian Electronic stock exchange (MTA) managed by Borsa Italiana S.p.A. and is part of the FTSE MIB index, which contains the stocks of the Italian large cap companies. Unipol is the Italian holding company at the head of the Unipol Insurance Group and the " ultimate parent company", pursuant to the provisions contained in the Private Insurance Code and the related implementing provisions.

The Unipol Group operates in the following business segments:

a) insurance, divided into the following sectors:
   - insurance, in which the Group historically operates in the Non-Life and Life businesses; and
   - bancassurance;

b) finance, with regard to collective asset management, financial intermediation and the management of the recovery of non-performing loans;

c) real estate;

d) other activities, in which it carries out, on a residual basis, hospitality activities, medical clinic and agricultural sectors.

3.2 Internal control and risk management system of Unipol Gruppo

In designing its corporate governance system, UG has implemented the recommendations contained in the Corporate Governance Code of listed companies in its various editions over time[13], which constitute a "best practice" corporate governance model for Italian listed companies.

Pursuant to the in-force regulation[14], the Parent Company provides the Group with a corporate governance system appropriate to its structure, business model and nature, extent, and complexity of the risks the Group and its participating and subsidiary companies face.

The company's Board of Directors has ultimate responsibility for the corporate governance system, defining its strategic guidelines and ensuring overall consistency. In this context, the Board of Directors - inter alia - defines and reviews Group policies, defines the Group's organizational structure, as well as the assignment of duties and responsibilities to the operating units, ensuring that an appropriate separation of functions is implemented.

The Board of Directors, in relation to the provisions of IVASS Regulation no. 33/2016 of 6 December 2016, annually approves the Solvency and Financial Condition Report (SFCR) of the Group addressed to the market and a periodic report addressed to the Supervisory Authority (Regular Supervisory Report), which include quantitative and qualitative information on the Group; more specifically, activities and results, governance system, risk profile, solvency assessment, and capital management.

[13] Former Corporate Governance Code for listed companies approved in March 2006 by the Corporate Governance Committee and promoted by Borsa Italiana S.p.A., as amended. The Corporate Governance Code was last amended on 30 January 2020 and renamed the "Corporate Governance Code". The new Code became applicable starting from the first financial year after 31 December 2020.

[14] Reference is made in particular to IVASS Regulation No 38/2018.

In addition, the Board of Directors approves the strategic plan on information and communication technology (ICT Plan), including corporate cyber security, aimed at ensuring the existence and maintenance of an overall integrated and secure systems architecture from an infrastructural and application point of view, adapted to the needs of the company and the Group, and based on international, national, and sectorial standards, guidelines, and regulations.

The internal control and risk management system, a fundamental element of the Group's corporate governance system, consists of all the rules, procedures and organizational structures that aim to ensure the proper functioning and smooth running of the Company and the Group.

The internal control and risk management system is an integral part of the company and must involve all its sectors and structures, involving every resource, each for its own level of duties and responsibility, to guarantee constant and effective risk monitoring. All company Departments and Functions have their own role in verifying the operations carried out, according to different levels of responsibility.

The internal control and risk management system is defined in the Directives on the Group Corporate Governance System which define, among other things, the role and responsibilities of the parties involved, and are supplemented by the Fundamental Functions Policies.

The internal control and risk management system is set up according to the following guidelines:

- separation of tasks and responsibilities: competences and responsibilities are shared between the governance bodies and organizational units in a clear manner, in order to avoid gaps or overlaps that may affect company operations;
- formalization: the work of the administrative body and the delegated subjects must always be documented, to allow the control of management actions and decisions taken;
- integrity, completeness and fairness of the data stored: the data recording system and related reporting must ensure that adequate information is available on the elements that may affect the risk profile of the company and its solvency;
- independence of controls: the necessary independence of the control structures must be ensured in relation to the operational units.

The coordination procedures and information flows between the parties involved in the internal control and risk management system are described in the Key Function Policies as well as in the Regulations of the Board Committees.

This system is periodically assessed and reviewed, in relation to the evolution of business operations and the reference context.

In general, the corporate bodies[15] and the top management structures promote the dissemination of a control culture that makes staff aware of their role at all levels, also with reference to control activities and encourages the involvement of all company departments in the pursuit of corporate objectives.

In preparing this Model, the existing internal control and risk management system and pertaining procedures have been accounted for, as they contribute to criminal prevention measures.

[15] Corporate bodies include the Board of Directors, the Board Committees, the Chairman and the Board of Statutory Auditors, as well as the General Manager

In particular, UG operates on the basis of the following tools, that help to conceptualize and implement company decisions, also in relation to the offences that need to be prevented:

- Applicable Italian and foreign laws, including regulations;
- the Articles of Association;
- Charter of Values and Code of Ethics of the Unipol Group;
- the Corporate Governance Code;
- the system of self-regulation of company discipline, as set out in paragraph 3.3 below;
- the system of delegations and executive powers in place;
- the disciplinary and sanctioning system referred to in the National Collective Labour Agreement, Supplementary Contracts in force and the Workers' Statute.

The rules, procedures and principles referred to in the tools listed above are not reported in detail in this Model but are part of the broader system of organization and control that it intends to integrate.

3.3 Group's internal regulatory system (newly introduced paragraph)

Unipol Group has adopted an articulated system of self-regulation of corporate discipline, applicable to all Group companies, consisting of different types of corporate communication documents (the "DCA").

The main types of DCA are classified according to content and scope.

The DCAs approved by the Board of Directors of the Parent Company and/or Group Companies and addressed exclusively to employees are:

- Group Policies and Procedures
- Policies and Procedures applicable at single company level (Group Companies)

With reference to the remaining DCAs, those that are aimed at employees working for Group Companies are:

- Ordine di Servizio (known as “ODS”) that announce organizational changes;
- Disposizione Interna that are internal company provisions;
- Regola Operativa (known as “ROP”) that are operational rules;
- Procedura Tecnica di Settore (known as “PTS”) that are business specific technical procedures.

The DCAs that can be addressed both to employees working for Group Companies and to Sales Networks are:

- Comunicato (known as “COM”) that are official announcements;
- Circolare (known as “CIR”) that are company administrative orders;
- Testo Unico (known as “TU”).

Unipol Group has also defined a set of preventive checks, carried out by specific Company Functions, prior to the publication of DCAs, to ensure the adequacy of each document with respect to the matters within its competence.

All DCAs are published within the company intranet or other repository in place to allow them to be viewed by all recipients.

3.4 General Principles of control

In general, the Company's organizational system must comply with the fundamental requirements of:

- explicit formalization of rules of conduct;
- clear, formal and understandable description and identification of the activities, tasks and powers attributed to each function and to the different qualifications and professional roles;
- specific description of control activities and their traceability;
- adequate segregation of operational and control roles.

In particular, the following principles must be pursued:

Rules of conduct

- the existence of a Code of Ethics describing general rules of conduct that govern the activities carried out must be envisaged;
- the Company's reward and incentive systems must be designed to ensure consistency with the provisions of the law, with the principles contained in this Model, also providing for appropriate corrective mechanisms in the face of any deviant behaviour.

Definitions of roles and responsibilities

- internal regulations must outline the roles and responsibilities of organizational units at all levels, describing the activities of each structure;
- such regulations must be made available and known within the organization.

Internal procedures and rules

- sensitive activities must be regulated, in a coherent and appropriate manner, through corporate regulations, so that at all times it is possible to identify the operating methods used to carry out the activities, the related controls and the responsibilities of those who operated;
- a Process Owner must be identified for each business process, typically coinciding with the person in charge of the organizational structure responsible for the management of the activity itself.

Segregation of duties

- within each relevant company process, the functions or persons responsible for making decisions and its implementation must be separated from those who register it and from those who control it;
- those who take or implement decisions, those who must account for the decisions made and those who are required to perform the controls on them as established by law and by the procedures of the internal control system must all be different persons.

Authorization and signatory powers

- a system of delegated powers must be defined within which there is a clear identification and a specific assignment of powers and limits to the subjects who are allowed to commit for the Company and manifest its will;
- the organizational and signature powers (delegations, powers of attorney and related spending limits) must be consistent with the organizational responsibilities assigned;
- powers of attorney must be consistent with the internal system of delegated powers;

- mechanisms must be established for disclosing powers of attorney to Third Parties;
- the delegation system must identify, inter alia:
  - the requirements and professional skills that the delegate must possess by reason of the specific scope of operation of the delegation;
  - the operational procedures for managing expenditure commitments.
- powers must be delegated according to the principles of:
  - decision-making and financial autonomy of the delegate;
  - technical-professional suitability of the delegate;
  - autonomous availability of resources appropriate to the task and continuity of services.

Operational control and traceability

- operational controls and their characteristics (responsibility, evidence, frequency) must be formalised in procedures or other internal regulations;
- the documents relevant to the performance of sensitive activities must be properly formalized and bear the date of completion, acknowledgement of the document and the recognizable signature of the author; they must be stored in suitable locations for storage, in order to protect the confidentiality of the data contained therein and to avoid damage, deterioration and loss;
- the formalisation and approval of corporate acts and deeds and the relative authorization levels, development of operations, materials and registration, with evidence of their motivation and their purpose, must be reconstructed, to guarantee the transparency of the decision making process;
- the person in charge of the activity must produce and maintain adequate reports that contain evidence of the checks carried out and any anomalies identified;
- where possible, an ICT system must be adopted to guarantee correct and truthful allocation of each transaction, or a segment thereof, to the person responsible for it and to the other parties that participate in it;
- the system must not allow (untraced) modification of the records;
- documents concerning the Company's activities, and in particular documents or computer documentation regarding sensitive activities, must be archived and kept by the competent function, in such a way as to disallow subsequent modification, except with specific evidence;
- access to documents already archived must always be motivated and allowed only to persons authorized according to internal regulations, the Board of Statutory Auditors, the Audit, Risk Management and Compliance and Anti-Money Laundering Functions and the SB, within the limits of their authorizations;
- Outsourced processes, especially if they concern sensitive activities, must be carefully monitored.

3.5 Purpose and Scope of the Model

Recognizing that transparency and integrity are the pre-conditions to organizing the company's activity, UG has adopted an organization, management, and control model suitable for preventing unlawful misconduct by all recipients.

Notwithstanding the optional choice of such a model laid out by Decree, UG has decided to comply with its provisions by adopting a model.

The purpose of the OMM is, therefore, to provide a structured and organic system of prevention, dissuasion and control aimed at developing awareness in subjects who, directly or indirectly, operate in the

field of sensitive activities. In this way they can identify, in the event of unlawful misconduct, the consequences that may lead to sanctions not only for themselves, but also for the Company.

The Model adopted by the Company identifies the activities in which the risk of committing offences could, even theoretically, be envisaged. It intends to:

- create awareness, in all those who carry out, in the name, on behalf and in the interest of the Company, activities at risk of offence, as better identified in the Special Parts of this document, the possibility that they may incur, in the event of violation of the provisions contained in the OMM, an offense punishable by criminal and administrative sanctions, which can be imposed not only against them, but also against UG;
- condemn any form of unlawful conduct by the Company, as it is contrary not only to the provisions of the law, but also to the ethical principles adopted by the same;
- guarantee the Company, thanks to the control of activities at risk of crime, the concrete and effective possibility of intervening promptly to prevent the commission of the offences themselves.

The Model also aims to:

- introduce, integrate, raise awareness, disseminate and circulate at all company levels the rules of conduct and protocols for planning the formation and implementation of the Company's decisions, in order to manage and, consequently, avoid the risk of committing offences;
- inform all those who work with the Company that the violation of the provisions contained in the OMM will result in the application of specific penalties or the termination of the contractual relationship, without prejudice to any request for compensation if such conduct causes concrete damage to the Company;
- identify in advance the activities at risk of offences, with reference to the activities carried out by the Company;
- provide the SB with adequate powers in order to put it in a position to effectively supervise the effective implementation, constant functioning and updating of the Model, as well as to evaluate the maintenance over time of the solidity and functionality requirements of the OMM itself;
- guarantee the correct and protocol-compliant registration of all the Company's operations in the context of activities at risk of offences to make it possible to verify ex post the decision-making processes, their authorization, and their performance within UG. All in accordance with the principle of control expressed in the Confindustria Guidelines by virtue of which "every operation, transaction, action must be verifiable, documented, consistent and coherent";
- ensure effective compliance with the principle of separation of corporate functions, in accordance with the principle of control, according to which "no one can independently manage an entire process", so that the authorization to carry out an operation is under the responsibility of a person other than the one who accounts for it, executes it operationally or controls it;
- outline and circumscribe responsibilities in the formation and implementation of the Company's decisions;
- establish that the authorization powers are delegated in accordance with the organizational and managerial responsibilities assigned, that the delegations of power, responsibilities and tasks within UG are disclosed and that the acts with which powers, delegations and autonomy are conferred are compatible with the principles of preventive control;
- identify the methods for managing financial resources, such as to prevent the commission of offences;

- evaluate the activity of all subjects who interact with UG, within the areas at risk of committing offence, as well as the functioning of the Model, taking care of the necessary periodic updating in a dynamic sense, if the analyses and evaluations made it necessary to make corrections, additions, and adjustments.

Through the Model, in fact, a structured and organic system of control procedures and activities (ex-ante and ex post) is consolidated, which aims to reduce the risk of committing offences through the identification of sensitive processes and their related formal procedures.

Among the purposes of the Model there is, therefore, that of developing awareness among employees, corporate bodies, consultants in any capacity, collaborators and partners, who carry out, on behalf and in the interest of the Company, activities at risk of offence, to be able to incur, in the event of conduct that does not comply with the provisions of the Model, as well as the rules of the Code of Ethics and other company rules and procedures (as well as the law), in offences liable to criminal consequences not only for oneself, but also for the Company.

Furthermore, it is intended to effectively censure any unlawful conduct through the constant control activity of the SB on sensitive processes and the imposition, by UG, of disciplinary or contractual penalties.

3.6 Model and its structure

The preparation and updating of this OMM were preceded by a series of preparatory activities divided into different phases and all aimed at the construction of a risk prevention and management system, in line with the provisions of Legislative Decree 231/2001 and inspired by the rules contained therein and the principles and suggestions dictated in this regard by the ANIA and Confindustria Guidelines.

The phases in which the preparation and updating of the OMM are divided are briefly described below.

a. Preliminary phase

In this phase, aimed at preparing the supporting documentation and planning the detection activities, punctual analyses were carried out on the existing documentation (organization charts, process surveys, risk surveys and assessments, and controls) and dialogue with the corporate functions concerned. The target was to identify the subjects, top management, and subordinates, that needed to be involved in the subsequent phase of risk assessment and to describe the control system. In addition, the areas of activity (corporate areas, organizational areas, processes and operational sub-processes) in which there is a risk of committing the offences provided for by Legislative Decree 231/2001 (process/crimes matrix - see MACROPROCESSES table) were identified and, in order to facilitate the subsequent risk assessment phase, the possible ways in which illegal conduct could materialise were identified.

b. Risk mapping and controls phase

In this phase, also considering what is suggested by the Confindustria Guidelines, an in-depth survey of the overall organization of UG was carried out, i.e., a survey of the areas, sectors and offices, related functions and procedures, and external entities, in various ways related to the Company.

For each of these areas, detailed documentary analyses and interviews with top and subordinate figures involved in the activities examined were carried out, to identify offences that could potentially be committed, the ways in which these would materialise, the types of existing controls (e.g. those of an organizational nature related to the clear identification and segregation of responsibilities and functions; those of a procedural nature, related to the formalization of activities in internal rules; those deriving from ICT solutions through the provision of mandatory formal steps, etc.) and their effectiveness. In detail, we proceeded to:

- analyse the Company's operations with reference to the so-called "sensitive" processes in which offences may be committed pursuant to Legislative Decree 231/2001;

- describe, in the organizational context analysed, the positions and subjects involved, their responsibilities and their powers, distinguishing between "top management" or "subordinate" figures, as indicated in Legislative Decree 231/2001;
- identify and describe the offences that could be committed and the consequences they could have;
- identify and describe the possible unlawful misconduct of the activity in question, i.e., the practical ways in which offences could be committed;
- identify in a timely manner the existing controls (ex-ante and ex-post) and evaluate the alignment of the control structure with the dictates of Legislative Decree 231/2001 in terms of existence, effectiveness and efficiency of controls, existence of formalized procedures, adequacy of the system of delegations and powers of attorney, existence and adequacy of the disciplinary system.

The risk and control detection phase has allowed to identify the functions and the subjects involved in sensitive processes, their responsibility, as well as the control systems adopted for risk mitigation.

c. Risk assessment phase and controls

In this phase, for each of the sensitive processes, the degree of risk was assessed using the " Control and Risk Assessment" method :

- together with the person responsible for each process, the risk of criminal administrative offences being committed in this context, taking into account the degree of effectiveness and efficiency of the procedures and control systems existing within the process, suitable for criminal prevention measures;
- on the basis of these assessments, any critical issues, in terms of risk pursuant to Legislative Decree 231/2001, within each process have been determined;
- In relation to the risks identified and the related criticalities, the appropriate corrective actions were identified to reduce the level of criticality and improve the control system.

For this moment to represent a real opportunity for awareness and involvement, the entire evaluation process and the related evidence that emerged were shared with management.

To provide an adequate formalization of the surveys conducted, a specific information system adopted by the Group's Audit, Risk Management, Compliance and Anti-Money Laundering Functions is used. It allows to manage the risk mappings carried out pursuant to the Decree, in line with the models for surveying company processes and general assessment of operational risks, making possible:

- a single database for storing all the information collected;
- the assessment, on the basis of metrics agreed at Group level, of the actual level of risk on the individual areas subject to risks pursuant to Legislative Decree 231/2001;
- a risk assessment pursuant to Legislative Decree 231/2001;
- the management of an improvement plan resulting from the analysis conducted.

3.7 Definition of Protocols: identification and analysis of sensitive processes

Unipol Group has identified the sensitive processes in which the conditions, opportunity, or possibilities for potentially committing a crime referred to in Legislative Decree 231/2001 could arise (see table MACROPROCESSES).

With reference to these processes, the management and control procedures in place were therefore identified and any necessary implementations were defined, where deemed appropriate, in compliance with the following principles:

- functional segregation of operational and control activities;
- documentability of risky operations and controls put in place to prevent offences from being committed;
- distribution and attribution of authorization and decision-making powers, competences and responsibilities, based on principles of transparency, clarity and verifiability and consistent with the activity actually carried out;
- access security and traceability of financial flows.

This detection process, to operate effectively, must be carried out continuously or in any case carried out with an adequate frequency and must be reviewed with particular attention in the face of corporate changes (e.g., opening of new offices, expansion of activities, acquisitions, reorganizations, changes in the organizational structure, etc.), or the introduction of new offences.

3.8 Definition of ethical principles

UG has adopted the Charter of Values and the Code of Ethics, which constitute the value framework of Unipol Group. The following five principles drive the Charter of Values:

- Accessibility: promotes mutual availability and dialogue, thus generating greater organizational effectiveness;
- Forward-Thinking: encourages the ability to correctly interpret market signals by anticipating trends, generating continuity in results and developing profits with a view to "enhanced" sustainability. Forward-Thinking allows to combine and encourage improvement, environmental aspects, economic and social requirements that allow the company to move forward in the long term;
- Respect: encourages attention to the needs of all stakeholders, generating quality of service and mutual recognition;
- Solidarity: encourages teamwork and trust in the rules, generating management efficiency;
- Responsibility: drives professional reliability, which allows to answer for one's actions in the times and in the manner defined by the rules of the sector, the market, and its corporate ethics.

The Group Code of Ethics has the following characteristics:

- it is principles-based, i.e. it refers to principles and doesn't describe conducts
- its structure inherits both the structure and the contents of the Charter of Values; it is inspired by an educational approach;
- it adopts special "restorative justice" devices aimed at identifying conducts capable of reinstating, in the ways deemed most appropriate, the status quo before the violations were committed.

The Ethics Officer of the Unipol Group has been appointed as a proactive reference figure to whom stakeholders can turn to obtain opinions and/or advice regarding the correct application of the Code of Ethics and as a collection and filtering center for any reports of violations.

The Code of Ethics must find ways to ensure compliance by all those who work in the orbit of the Unipol Group. A commitment to respect the values refers to all the Group's stakeholders, identified in the following six categories:

- shareholders and investors;
- employees and collaborators;
- customers;

- suppliers;
- civil community;
- future generation.

The reference principles that drive this Model are therefore integrated with those of the Charter of Values and the Code of Ethics adopted by UG, even if the Model, implementing the provisions of Legislative Decree 231/2001, has a different scope and purpose than the Code of Ethics.

From this point of view, in fact, it is appropriate to specify that:

- the Code of Ethics has a general application, as it contains a series of principles of "corporate ethics" that UG recognizes as its own and to which it requires observance from all those who cooperate in the pursuit of company purposes;
- this Model responds to and satisfies, in accordance with the provisions of Legislative Decree 231/2001, the need to prepare a system of internal rules aimed at preventing specific types of offences.

3.9 The procedure for adopting the Model

Although the adoption of the Model is optional and not mandatory by law, the Board of Directors of the Company, in accordance with its corporate policies, has decided to proceed with the adoption of the Model as of March 19th, 2009.

At the same time as the adoption of the Model, the SB was appointed with the duty of supervising the functioning and observance of the Model, as well as ensuring it is up to date (see chapter 5).

Subsequent amendments and material additions to the Model are referred to the Board of Directors of Unipol Group, subject to the opinion of the SB, the Model being a "document issued by the management body" in accordance with the provisions of art. 6 of Legislative Decree 231/2001. The SB can also propose changes to the Model.

In the Board meeting of 28 September 2023, the Board of Directors of UG updated this Model and expressly stated its commitment to remain compliant with it. The Board of Statutory Auditors has taken note of this Model and has also formally committed to remaining compliant with this Model.

Regarding the scope of the OMM, it should also be noted that certain activities are outsourced by Unipol Group to its subsidiary UnipolSai.

The extension of this Model to the outsourcer shall be considered limited to the performance of sensitive processes carried out by the same in the name and on behalf of UG and takes place based on contractual agreements governing relations between the Company and the outsourcer, providing for an accurate discipline of controls by the Company and the related periodic reporting activities.

In any case, UnipolSai has adopted its own Organizational Model pursuant to Legislative Decree 231/2001 which includes and coordinates numerous ethical, organizational, managerial and control procedures.

In this circumstance, UG further relies on the above for the conception and implementation of its own control system pursuant to and for the purposes of Legislative Decree 231/2001.

Employees and suppliers are required to declare they fully acknowledge the contents and requirements contained in Legislative Decree 231/2001 and commit to comply with it, providing specific information in the context of the contract.

4 THE COMPANY PROCESSES EXPOSED TO OFFENCES AS PER LEGISLATIVE DECREE NR 231/2001

Following a detailed analysis of business operations and risk mapping pursuant to Legislative Decree 231/2001, UG has identified the relevant business processes for the purposes of Legislative Decree 231/2001, i.e. the so-called “sensitive” processes.

From the analysis carried out, the categories of crime that could potentially be committed in the context of sensitive business processes are the following:

1. Crimes in relations with the Public Administration;
2. Corporate offences;
3. Crimes and administrative offenses of insider dealing, market manipulation and rigging;
4. Receiving stolen goods, money laundering, self-laundering and crimes with the purpose of terrorism or subversion of the democratic order;
5. Computer crimes;
6. Manslaughter or serious or very serious injuries committed with violation of the occupational health and safety standards;
7. Organized crimes and cross-border offences;
8. Environmental offences;
9. Copyright infringement;
10. Employment of illegally staying third country nationals;
11. Incitement to not make statements or make false statements to the judicial authority;
12. Illicit brokering and labor exploitation;
13. Fraud in sports competitions;
14. Tax offences.

Below is a table that intersects between crime categories listed above and the company sensitive processes, appropriately grouped into broader categories called "macro-processes", in which the crimes could be committed.

MACROPROCESS	Offences in relations with the Public Administration	Corporate offences	Market Abuse	Receiving stolen goods, terrorism	Computer crimes	Manslaughter/ grievous bodily harm	Organized crime and cross-border offences	Environmental offences	Copyright infringement	Illegal employment	False or no testimony / statements	Illicit brokering and labor exploitation;	Sports fraud	Tax offences
Asset management	✔	✔	✔	✔			✔							✔
Cash management	✔	✔	✔	✔			✔						✔	
Purchasing Management & Procurement	✔	✔		✔		✔	✔	✔		✔		✔	✔	✔
Accounting and Financial Statements		✔	✔	✔			✔							✔
Tax management	✔	✔		✔			✔							✔
Strategic Marketing and communications	✔	✔					✔		✔				✔	
IT systems management	✔	✔			✔		✔		✔					
HR management and administration	✔	✔					✔			✔	✔	✔	✔	✔
Staff training	✔	✔				✔	✔						✔	
Safety in the workplace	✔	✔				✔	✔					✔		
Property management	✔	✔				✔	✔	✔		✔		✔	✔	
Legal advisory and litigation	✔	✔	✔	✔			✔				✔			
Corporate governance and supervisory authority relations		✔	✔				✔							
Anti-terrorism				✔			✔							
External communication and Investor relations			✔				✔							
Risk Management		✔	✔				✔							
Group Coordination and management		✔					✔							
Audit		✔												
Compliance		✔												

5 THE SUPERVISORY BODY

5.1 Identification, requirements, and appointment of Supervisory Body

a) Appointment and establishment of the Supervisory Body

The Decree provides for the establishment of a Supervisory Body within the Entity with autonomous powers of initiative and control, which is assigned the duty of supervising the functioning and compliance with the Model and updating it.

In compliance with the provisions of art. 6, paragraph 1, lett. b) of Legislative Decree 231/2001, the Company identifies the SB as a collegial body, composed of a maximum of five members, identified as follows:

- all members of the Control and Risk Committee, all independent non-executive directors;
- the additional member(s) is/are one/two external professional(s) with adequate skills and professionalism or a member of the company's Top Management responsible for the Audit or the Compliance and Anti-Money Laundering Functions.

In line with the provisions of the law, this composition ensures that the requirements with respect to autonomy and independence, professionalism and operational efficiency of the SB are ensured.

The compensation attributed to the members of the SB is determined by the Board of Directors at the time of appointment and remains unchanged for the entire term of office.

In addition, the Board of Directors, annually and upon proposal of the SB, approves the forecast of expenses, including extraordinary expenses, necessary for carrying out the supervisory and control activities envisaged by the Model, as well as the final balance of any expenses incurred in the previous year.

b) Fit-and-proper eligibility requirements of the members of the Supervisory Body

The members of the SB must be in possession of fit-and-proper requirements according to the specific duties entrusted to them.

The members of the Body must certify that:

- they have no marriage, kinship or family relationship up to and including the 4th degree, with members of the decision-making bodies of the Entity or the Independent Auditors, or with the auditors appointed by the Independent Auditors, or among themselves;
- they are not executive members of the decision-making body of the Entity or the Independent Auditors;
- they have no actual or potential conflicts of interest with the Entity such as to jeopardise their independence;
- they have not performed, at least in the previous three years, administrative, management or control function activities in companies subject to bankruptcy, compulsory liquidation or equivalent procedures or in companies operating in the credit, financial, securities and insurance sectors subject to extraordinary administrative procedures;
- they have not been subjected to preventive measures ordered by the judicial authority pursuant to Legislative Decree 159/2011 and subsequent amendments, without prejudice to the effects of rehabilitation;
- they have not been convicted with a sentence, even if not final, for crimes provided for by Legislative Decree 231/2001, without prejudice to the effects of rehabilitation.

The members of the SB commit to immediately notify the Company of any event that involves the loss, even temporary, of the requirements described above.

Prior to the appointment of the person concerned in the role of member of the SB, and subsequently, on an annual basis, the Board of Directors assesses the existence of the above-mentioned fit-and-proper requirements.

The requirement for professionalism implies that the members of the SB have competence in legal, economic, and financial matters, to guarantee the effectiveness of the supervisory and proactive powers delegated to them.

The professional and personal profile of each member of the SB must also be suitable to guarantee authority, impartiality of judgment and ethics of conduct.

The failure to meet the above-mentioned requirements, or the occurrence of causes for incompatibility during the mandate will result in forfeiture of office. In this case, the Board of Directors shall promptly appoint a new member, in compliance with the principles indicated. The member thus appointed will remain in office until the end of the mandate of the SB.

c) Autonomy, Independence

The SB must be endowed, in its collegiality, with specific requirements of autonomy, independence and professionalism.

The above-mentioned requirements presuppose that the Body:

- carries out its core activities with continuity of action;
- is composed of individuals whose personal circumstances and/or interests do not conflict with the assigned task or compromise the high degree of authority required to exercise their independence in judgment and assessment.
- reports on its activities exclusively to the Board of Directors and maintains contacts with the Control and Risk Committee, the Board of Statutory Auditors and the Independent Auditors.

d) Duration in office and causes of termination of the members of the Supervisory Body

The term of office of the SB is equal to that of the Board of Directors.

The Supervisory Body (SB) is appointed at the first available meeting of the Board of Directors following the Shareholders' Meeting during which the Board of Directors is appointed and serves until the Board of Directors is renewed.

The termination of the office or company role held by any appointed internal member(s) determines the termination of office of member of the SB. In this case, the Board of Directors shall promptly appoint a new member.

A member of the SB may be revoked exclusively for just cause (i.e., for gross negligence in the exercise of office), by resolution of the Board of Directors, having heard the mandatory but non-binding opinion of the Board of Statutory Auditors.

5.2 Functions and powers of the Supervisory Body

The SB is generally entrusted with the task of supervising:

- the effectiveness and adequacy of the OMM in relation to the corporate structure, the ability of the same to prevent offences referred to in Legislative Decree 231/2001, also in terms of suitability and adequacy of the contents. This activity takes the form of an assessment of the provisions of the Model in relation to the pro tempore legislation in force, best practices and jurisprudence on the liability of collective bodies;
- the observance of the Model by the recipients: employees, corporate bodies and, within the limits provided therein, collaborators and suppliers;
- the possibility of updating the Model, where there is a need to adapt it to changed company conditions and/or regulations, requesting the competent bodies to do so to this end.

The SB regulates its operational rules, formalizing them in a special regulation, approved independently.

The meetings of the SB and the meetings with the other corporate control bodies must be recorded and copies of the minutes kept by the Body itself.

On a more operational level, the SB is entrusted with the task of:

- organizing the adoption of the procedures established for the implementation of the control system;
- promoting initiatives aimed at spreading awareness and understanding of the principles set out in the OMM;
- collecting, processing and storing relevant information regarding compliance with the Model;
- coordinating with the competent company functions (also through special meetings) for the appropriate monitoring of activities in sensitive areas. To this end, the SB is kept constantly informed about the evolution of activities in the above-mentioned risk areas. Management must also report to the SB any instances of company activity exposing the latter to a potential risk of offence.
- coordinating with the corporate function responsible for the control of outsourced activities (so-called Link Auditor), for the appropriate monitoring of sensitive outsourced activities. To this end, the SB is kept periodically informed about the above-mentioned activities;
- requesting, where deemed appropriate, specific comparisons or exchanges of documents with the independent auditors;
- assessing the appropriateness of the required documentation, in accordance with the guidelines stipulated in the protocols and control system action plans. Specifically, reports to the SB must have a mutually agreed-upon format, encompassing the most noteworthy activities undertaken, including any prepared action plans. Moreover, documentation updates must be accessible to facilitate subsequent inspections.
- conducting internal investigations, in agreement with the competent company departments, to assess alleged violations of the requirements of the OMM;
- coordinating with the various Function Managers for the various aspects related to the implementation of the Model (staff training, needs for interpretation of the relevant legislation);
- assigning to third parties, in possession of the specific competence necessary for the best execution of the assignment, any tasks of a technical nature;
- arranging special meetings with the company departments concerned to assess the need to update the OMM,

Considering the responsibilities assigned and the specific professional content required, the SB:

- in carrying out its tasks, relies on the Audit and the Compliance and Anti-Money Laundering Function, from which it can also request specific insights and/or analysis;

- is informed by the Audit and the Compliance and Anti-Money Laundering Function of the results of the control activities carried out that have a relevance for purposes related to Legislative Decree. 231/2001;
- may require the support of other company functions, as well as external consultants.

To fully implement the tasks entrusted to it and to ascertain any violations of the Model, the SB is granted specific powers of initiative and control that can be exercised in all sectors of the Entity, including the decision-making body and its members, as well as towards collaborators, suppliers and consultants of the same.

For the above-mentioned purposes, the SB may carry out checks, request information, carry out inspections, access both premises and data, archives and documentation, in coordination with the defined company units.

By way of example, the SB has the right to carry out targeted inspections, even without prior notice, on certain operations or specific acts carried out by Unipol, especially in the context of sensitive activities. The conclusions of such inspections must be summarized in a report to the competent corporate bodies.

At the end of the above-mentioned verification activities, the SB is given the task of monitoring the correct implementation of the procedural requirements necessary to issue disciplinary measures against those responsible for violations of the Model.

The exercise of the above-mentioned powers must take place within the limit strictly functional to the performance of the tasks of the SB, which does not in any way have management powers.

The activity carried out is summarized in the annual report to the Board of Directors which also highlights any critical issues encountered and improvements to be implemented.

5.3 Reporting of the Supervisory Body to Top Management

As the SB may be called upon at any time, well in advance, by the Board of Directors to report on the functioning of the Model or on specific situations, the following line of reporting to the Board of Directors is assigned to the SB, in full compliance with the Legislative Decree 231/2001 as well as the prevailing doctrine, and may submit a request to that effect:

- at least annually, the SB sends the Board of Directors a written Report on the activities carried out and the activities planned for the following year. This report includes:
  1. the activity carried out by the SB;
  2. any critical issues that have emerged, both in terms of conduct or events within the Institution, and in terms of the effectiveness of the OMM;
  3. any suggestions for improvement.

Upon occurrence of situations that the SB considers extraordinary, or of reports of an urgent nature pursuant to the regulations referred to in Legislative Decree 231/2001, the SB prepares an immediate communication to the decision-making body.

5.4 Reporting to the Supervisory Body: general and mandatory information

Among the requirements that the Model must meet to be considered suitable for preventing offences included among the cases referred to in Legislative Decree. 231/2001, Article 6 provides for the establishment of "reporting obligations towards the body responsible for supervising the functioning and compliance with the models". Reporting is the tool that enables the monitoring of the effectiveness of the Model and ascertains ex-post the causes that made possible the occurrence of any crime.

To meet these needs, there are two types of reporting flows:

- periodic;
- ad hoc.

The periodic reporting varies depending on the company's activities, enabling the monitoring of the progress of the analyzed activity and the effectiveness of the associated control measures, highlighting:

- critical issues:
  - the most significant events, also identified on the basis of qualitative and quantitative thresholds, in terms of potential risk of committing crimes and any anomaly indicators;
  - the reports prepared by the heads of the Audit, Compliance and Anti-Money Laundering Functions, as well as by the Financial Reporting Officer, who, as part of his verification activity, identifies any omissions or critical profiles pursuant to Legislative Decree 231/2001;
  - periodic disclosure concerning the use of training courses on Legislative Decree 231/2001 by employees and top management;
  - periodic disclosure concerning organizational interventions aimed at the effective implementation, at all company levels, of the Model;
  - disclosure relating to any (i) organizational changes (by way of example introduction or removal of business lines), (ii) regulatory developments relating to Legislative Decree 231/2001 that may lead to deficiencies and the need to make changes to the OMM;
- periodic disclosure from the areas executing the most significant so-called "sensitive" processes, even in the absence of specific problems;
- the design aspect:
  - disclosure containing any problems that have arisen with reference to the application of prevention protocols (internal rules) provided for by the Model;
  - disclosure relating to any facts, anomalies, violation that have emerged in relation to the management of company information systems;
  - the SB also acquires the outcome of the verification activities carried out by Audit with reference to the processes wholly or partly outsourced to companies belonging to the Group.

Ad hoc reporting includes anomalies or atypicality found in the context of the available information, i.e. consisting of investigations focused on individual facts that may have given rise to offences or in any case indicative of anomalies; these may consist of:

- disclosure on the possible initiation of legal proceedings relating to suspected offences included in the cases referred to in Legislative Decree 231/2001;
- disclosure containing information on inspections by Supervisory Authorities (Consob, Italian Competition Authority, etc.) or by Public Officials with control functions (Guardia di Finanza, etc.);
- reports containing information on any inspections and / or facts / anomalies / violations that have emerged in the field of occupational health and safety pursuant to Legislative Decree 81/2008;
- reports of violations of the Model committed by employees or top management;
- reports of violations of the Model committed by non-employees.

The SB endeavors, in agreement with the company functions, to identify the information necessary for its appropriate performance of the supervisory role it has over the functioning and observance of the Model, and which must be sent to it (including the relative periodicity).

All the information, notification and reports provided for in this Model are kept by the SB for a period of 10 years.

Periodic exchanges of information are planned between the SB and the Board of Statutory Auditors of the Company, as well as with the Independent Auditors and the Control and Risk Committee.

5.5 Communications by the Supervisory Bodies of Group Companies

To ensure effective and efficient coordination of supervisory activities, and to ensure they are carried out in full compliance with the principles of autonomy and independence as previously declined, the SB communicates annually with the Unipol Group Supervisory Bodies.

In the case of activities wholly or partially outsourced within the Group, the Body may activate specific forms of cooperation with similar Bodies operating within the Unipol Group aimed at increasing the effectiveness of the supervisory activities of each Body on transversal processes or activities.

5.6 Confidentiality obligations of the Supervisory Body

The members of the SB must ensure that the information collected while holding their positions should be treated with the highest degree of confidentiality and refrain from using such information for purposes other than those relating to the discipline referred to in Legislative Decree 231/2001. Any information in their possession is treated in accordance with the pro tempore legislation in force.

5.7 Reporting of the offences or violations of the Model

In accordance with Article 6, paragraph 2-bis[16], of Legislative Decree 231/2001, the Model provides for an internal system for reporting violations (i.e. whistleblowing) that allows:

- shareholders;
- persons with administrative, management, control, supervisory or representative functions, even if these functions are exercised merely by way of fact;
- employees of the Company, including any employees posted by other companies, temporary workers and apprentices;
- self-employed workers, including occasional workers, freelancers, consultants, volunteers and trainees (paid and unpaid), who work at the Company;
- workers and collaborators who carry out their work with suppliers of goods or services, contractors or subcontractors used by the Companies in perimeter;

to communicate information, including well-founded suspicions, concerning, inter alia, significant illegal conduct pursuant to Legislative Decree 231/2001 or violations of the OMM of which they have become aware in the context of their work, as well as elements concerning conduct aimed at concealing such violations. This is to protect the public interest and the integrity of the entity.

The internal system for reporting violations is formalised in a specific Group procedure (the "Procedure")[17], approved by the Company's Board of Directors.

[16] Article introduced by Law 30 November 2017, n. 179 " Provisions for the protection of whistleblowers reporting offences or irregularities of which they have become aware in the context of a public or private employment relationship".

[17] Procedure for reporting violations (c.d. "whistleblowing").

The Procedure identifies (i) the person or the autonomous function with specifically trained personnel responsible for receiving, examining and assessing whistleblowing reports (the "Principal/ Alternative Designated Structure[18]") and (ii) the means through which they can be transmitted, in writing, orally or by an in-person meeting.

The reporting channels and means referred to above shall ensure the confidentiality of the identity of the whistleblower, the person involved or mentioned, as well as the content of the report and related documentation in the reporting management activities.

Reports relating to significant unlawful conduct pursuant to Legislative Decree 231/2001 or violations of the Model are brought to the attention of the governance bodies by the Responsible Function, according to the rules set out in the Procedure. This also serves to collect any information from the former. The Responsible Function shall keep the SB constantly updated on the progress of the report.

UG undertakes to protect whistleblowers- with the exclusion of unfounded reports made with willful misconduct or gross negligence[19] - from any conduct, act or omission, even attempted or threatened, carried out as a result of the report and which causes or may cause unfair damage to the whistleblowers, directly or indirectly.

In this regard, reference should be made to paragraph 6.9 that states the penalties applicable to those who violate the protections set for the whistleblower.

The whistleblower who believes he has suffered retaliation or discrimination can act in the manner and form provided for in Article 19, paragraph 1 of the Whistleblowing Decree.

Pursuant to art. 19, paragraph 3 of the Whistleblowing Decree, termination and any other retaliatory measure or discrimination adopted against the whistleblower are null and void. It is the employer's responsibility, in the event of legal or administrative proceedings or in any case of out-of-court disputes concerning the ascertainment of the conducts, acts or omissions prohibited by art. 17 of the Whistleblowing Decree, to demonstrate that these measures are based on reasons unrelated to the report itself.

Please refer to the Procedure, published in the dedicated section of the Company's website[20], for further details.

[18] The report can be addressed to the Company's Alternative Responsible Structure if the members of the Main Responsible Structure are hierarchically or functionally subordinate to any reported person or are themselves the alleged perpetrators of the violation to have a potential interest related to the report, which could compromise its impartiality and independence of judgment.

[19] Under Article 20(3) of the Whistleblowing Decree "(...) when the criminal responsibility of the whistleblower is ascertained, even by judgment of first instance, for defamation or slander or for the same crimes committed with the complaint to the judicial or accounting authority, or civil liability, for the same reason, in cases of wilful misconduct or gross negligence, the protections referred to in this Chapter are not guaranteed and a disciplinary sanction is imposed on the whistleblower or complainant".

[20] https://www.unipol.it/it

6 DISCIPLINARY MEASURES AND PENALTIES

6.1 General Principles

Pursuant to art. 6, paragraph 2, letter e) and 7, paragraph 4, letter b) of Legislative Decree 231/2001 an adequate sanctioning system must be set up in case of violation of the provisions of the OMM.

Failure to comply with the provisions of the Model and the Code of Ethics, damaging the relationship between UG and its "stakeholders", entails, as a consequence, the application of disciplinary sanctions against the interested parties, regardless of the possible exercise of criminal prosecution by the judicial authority.

The rules of conduct imposed by this MOG are adopted by UG in full autonomy and regardless of the type of offense that violations of the Model itself may determine.

6.2 General Criteria for the imposition of penalties

The type and extent of the penalties applied in each case of violation detected will be proportionate to the seriousness of the violations and, in any case, defined based on the following general criteria:

- subjective evaluation of conduct according to the type of offense;
- seriousness of the obligations violated;
- level of hierarchical and/or technical responsibility of the person involved;
- possible sharing of liability with other parties who have contributed to causing the crime;
- presence of aggravating or mitigating circumstances with particular regard to professionalism, previous work performance, disciplinary measures, circumstances in which the act was committed.

Any disciplinary sanctions, regardless of the existence and / or the outcome of criminal proceedings, must be inspired by the principles of timeliness, immediacy, and fairness.

6.3 Scope

Pursuant to the combined provisions of Articles. 5, lett. b) and 7 of Legislative Decree 231/2001, the penalties provided for by the National and Supplementary Collective Labour Agreements, as well as by law, may be applied against UG personnel who engage in disciplinary offenses, depending on the severity, deriving from:

- failure to comply with the provisions of the Model;
- lack or untruthful recording of the activity carried out in relation to the documentation, conservation and control of the acts required by company procedures and regulations and protocols;
- failure of hierarchical superiors to supervise the behavior of their subordinates;
- violation of the reporting obligations towards the SB;
- violation and/or circumvention of the control system, put in place by subtracting, destroying or altering the documentation required by the procedures, or preventing the control or access to information and documentation to the person in charge, including the SB.

For the purposes of applying penalties, the seriousness of disciplinary offences will be assessed by the Human Resources and Organisation Area from time to time based on the principles contained in the previous paragraph.

6.4 Measures against employees

The violation of the provisions of the Model may constitute a breach of contractual obligations, with all legal consequences, also with regard to any compensation for damages, in compliance, in particular, with articles 2104, 2106and 2118 of the Civil Code, art. 7 of Law no. 300/1970 ("Workers' Charter"), of Law n°. 604/1966 and subsequent amendments on individual dismissals, as well as collective labour agreements, and even art. 2119 of the Italian Civil Code, which provides for the possibility of dismissal for just cause.

The penalties provided for by the National Collective Labour Agreement (CCNL) of the sector will be applied. Their adoption must take place in compliance with the procedures provided for by the Workers' Charter, as well as by the above-mentioned CCNL.

The detection of the above-mentioned violations, disciplinary proceedings and the application of penalties are the responsibility of the Human Resources and Organisation Area.

6.5 Measures against managers

Failure by managers to comply with the provisions of this Model, depending on the seriousness of the violations and considering the trusted nature of the employment relationship, may result in:

a) Delivery of a letter of reprimand

This measure is applied when conducts are identified, in the performance of activities in risk areas, that constitute minor violations with respect to the provisions of the Model.

b) Termination of the employment

This measure is applied when conducts are identified, in the performance of activities in risk areas, that constitute serious violations with respect to the provisions of the OMM.

6.6 Measures against Directors

In the event of violation of the provisions by a Board member, the SB informs the Board of Statutory Auditors and the entire Board of Directors, which will take the appropriate initiatives provided for by current legislation (liability action).

6.7 Measures against Statutory Auditors

The SB informs the Board of Statutory Auditors and the Board of Directors if a violation of the Model has been committed by a Statutory Auditor. The Board of Statutory Auditors, with the abstention of the person involved, proceeds with the necessary investigations and, after consulting the Board of Directors, takes appropriate measures. If the violation is attributable to more than one Statutory Auditor, it is communicated only to the Board of Directors for the adoption of appropriate measures.

6.8 Measures against collaborators and suppliers

With regard to all those who work as collaborators and suppliers of UG, the following provisions apply: any conduct carried out by collaborators and suppliers in contrast with the guidelines indicated by the Model and the Code of Ethics, may determine the termination of the contractual relationship, in accordance with the provisions of the specific contractual clauses included in the letters of appointment or contractual agreements and without prejudice to any request for compensation if such conduct causes tangible damage to the Company.

6.9 Measures to protect the internal whistleblowing system

Pursuant to art. 21 paragraph 2 of the Whistleblowing Decree and in compliance with the provisions of paragraph 2-bis[21], letter d), of Article 6 of Legislative Decree. 231/2001, the following conducts are considered equivalent to failure to comply with the provisions of this Model and therefore subject to the same penalties :

- violation of the protection measures of whistleblowers set forth in chapter 5.6 of the Model governed by the Whistleblowing Procedure;
- commission of other offences referred to in art. 21 paragraph 1[22] of the Whistleblowing Decree.

[21] Paragraph amended by the Whistleblowing Decree

[22] "Without prejudice to the other profiles of responsibility, ANAC applies the following administrative pecuniary sanctions to the person responsible: a) from 10,000 to 50,000 euros when it ascertains that retaliation has been committed or when it ascertains that the report has been hindered or that an attempt has been made to hinder it or that the confidentiality obligation referred to in Article 12 has been violated; b) from 10,000 to 50,000 euros when it ascertains that no reporting channels have been established , that no procedures have been adopted for the execution and management of reports or that the adoption of such procedures does not comply with those referred to in Articles 4 and 5, as well as when it ascertains that the verification and analysis of the reports received has not been carried out; c) from 500 to 2,500 euros, in the case referred to in Article 16, paragraph 3, unless the reporting person has been convicted, even at first instance, for the crimes of defamation or slander or in any case for the same crimes committed with the complaint to the judicial or accounting authority ."

7 THE DISSEMINATION OF THE MODEL AMONG THE ADDRESSES

To ensure the effectiveness with this Model, it is necessary to ensure correct knowledge and disclosure of the rules of conduct contained therein to both employees and top management. This objective concerns all company resources, whether they are resources already present in the company or those to be added. The level of training and information is implemented with a different degree of depth in relation to the level of involvement of the resources themselves in sensitive activities.

The SB, as far as it is competent, supervises and integrates the information and training system in collaboration with the Human Resources and Organization Area.

7.1 Information and training for employees and Top management

The distribution of the Model is carried out through publication on the company intranet website, accompanied by general information relating to Legislative Decree 231/2001.

The adoption of the Model and its updates are communicated to employees at the time of adoption itself or updating by company communication notified by e-mail (or similar electronic tool) to all employees in the workforce by the competent structure.

New hires are given an information kit, which provides them with the knowledge considered of primary importance. This information kit contains, in addition to the documents usually delivered to the newly hired, the Code of Ethics, the Charter of Values, the Model and Legislative Decree 231/2001.

In addition to the awareness-raising activities already carried out by the Group and directed towards all employees including top management, additional training and information sessions are carried out aimed at spreading knowledge on Legislative Decree 231/2001. These sessions are customized in their content and delivery methods (ie online or in-person), depending on the skills and needs of the trainees:

- classroom training is provided to front lines and operational managers, with a presentation for the benefit of the above-mentioned subjects during which:
  - they are informed about the provisions of Legislative Decree 231/2001;
  - they are made aware of the importance for the Company to adopt a governance and risk control system;
  - the structure and main contents of the Model adopted are described, as well as the methodological approach followed for its implementation and updating;
  - the conduct to be followed in terms of communication and training of their subordinates is described, in particular of the personnel operating in the company areas considered sensitive;
  - the conduct to have with the SB is illustrated, regarding communication, reporting and collaboration when carrying out their supervisory and monitoring activities of the OMM.
- information is provided to employees operating in procedures sensitive to the crimes covered by Legislative Decree 231/2001 to foster awareness on behalf of department managers to the potential crimes their subordinates could commit. The appropriate conduct to be observed, the consequences deriving from failure to comply with them and, in general, with the Model adopted by the Company is provided;

- online training allows to reach all employees indiscriminately on the company intranet site, with the aim of spreading knowledge of Legislative Decree 231/2001 and the MOG.

Participation in the training programs described above is mandatory. At the end of the training courses, specific learning tests and a final certificate is issued.

Failure to participate in training programs in the absence of justified reason is liable to be assessed from a disciplinary point of view.

Verification of actual use is entrusted to UnipolSai's Unica - Employee Training and Distribution Networks function, which reports to the SB.

7.2 Information for collaborators and suppliers

Collaborators and suppliers are informed of the content of the Model, also by referring to the publication of the same on the Company's website and of the need for UG that their conduct complies with the provisions of Legislative Decree 231/2001.

Collaborators and suppliers are required to issue to UG a declaration certifying full knowledge of the contents and requirements contained in Legislative Decree 231/2001 and the commitment to comply with it, providing specific information in the context of the contract.