ORGANISATION, MANAGEMENT AND CONTROL MODEL

PURSUANT TO LEGISLATIVE DECREE NO. 231 OF 8 JUNE 2001

Approved by the Board of Directors of Telepass S.p.A. on 28 May 2025

SUMMARY

DEFINITIONS

Telepass or the Company:	Telepass S.p.A.
Mundys	Mundys S.p.A.
Telepass Group or **the Group**	Telepass and the companies controlled by it pursuant to Article 2359, paragraphs 1 and 2, of the Italian Civil Code.
Mundys Group	Mundys and the companies controlled by it pursuant to Article 2359, paragraphs 1 and 2, of the Italian Civil Code.
Decree or **Legislative Decree 231/2001**	Legislative Decree No. 231 of June 8, 2001.
Confindustria Guidelines	Guidelines for the drafting of organizational, management, and control models pursuant to Legislative Decree No. 231/2001, issued by Confindustria on November 3, 2003, and subsequently updated.
Model or **MOG**	Organizational, Management, and Control Model adopted by the Company pursuant to Legislative Decree No. 231/2001 to prevent the commission of the offenses provided for under the Decree.
Code of Ethics	The Code of Ethics of the Mundys Group, which outlines the values and conduct principles guiding the Company's business activities.
Offenses or **predicate Offenses**	Offenses deemed relevant pursuant to Legislative Decree No. 231/2001.
Risk Area	Business activities considered potentially at risk for the commission of offenses under Legislative Decree No. 231/2001.
Control Measures	The set of norms, protocols, and corporate provisions aimed at preventing criminal risks, including but not limited to procedures, operational rules, manuals, forms, and employee communications.
Supervisory Body or **SB (*Organismo di Vigilanza*)**	The internal body tasked with overseeing the functioning, effectiveness, and compliance of the Model, as well as its updating, pursuant to Article 6,

	paragraph 1, letter b) of Legislative Decree No. 231/2001.
Corporate Bodies	The Board of Directors and the Board of Statutory Auditors of Telepass.
Top Management	Pursuant to Article 5, paragraph 1, letter a) of Legislative Decree No. 231/2001, individuals holding representation, administration, or management roles in the entity or one of its organizational units with financial and functional autonomy, as well as individuals who, de facto, manage or control the entity.
Subordinate Individuals	Pursuant to Article 5, paragraph 1, letter b) of Legislative Decree No. 231/2001, individuals subject to the direction or supervision of a member of Top Management.
Recipients	Those to whom the rules of conduct and ethical principles contained in the Code of Ethics, the Model, and the adopted Control Measures are addressed.
Third-Party Recipients	Parties engaging in commercial and/or financial relations of any kind with the Company who are contractually bound to comply with the ethical principles and/or the Model adopted by Telepass.
Public Administration (PA)	Public Administration entities, including their officials and individuals performing public service duties.
Collective Labor Agreement (CCL)	The Collective Labor Agreements applicable to the Company.
Whistleblowing	The system protecting employees or collaborators who report unlawful conduct encountered during their professional duties.
Reporting Team (*Team Segnalazioni*)	A collegial body responsible for managing reports. It comprises the heads of Telepass's organizational units in charge of Internal Audit, Human Resources, and Legal Affairs. The Reporting Team operates within Telepass and all companies controlled by it.

Reporting Procedure	The procedure governing information flows from Telepass organizational units to the Supervisory Body.
Criminal Code (c.p.)	The Italian Criminal Code.

GENERAL SECTION

INTRODUCTION

Legislative Decree No. 231 of June 8, 2001, as subsequently amended and supplemented, introduced into the legal system the "*Regulation of administrative liability of legal entities, companies, and associations, including those without legal personality*".

The Company, committed to ensuring fairness and transparency in conducting business and corporate activities to safeguard its market position, reputation, shareholder expectations, and employees' work, has:

a) adopted the Code of Ethics, the Anti-Corruption Policy, the Code of Conduct for the prevention of discrimination and the protection of the dignity of women and men, and the Telepass Group Whistleblowing Management Procedure, to regulate the proper conduct of its activities;

b) appointed, during the Board of Directors meeting on November 7, 2017, the Anti-Corruption Officer in compliance with the Mundys Group Anti-Corruption Policy;

c) deemed it appropriate to adopt and implement an Organizational, Management, and Control Model (MOG) designed to establish a structured system of rules and controls to pursue the Company's objectives in full compliance with applicable laws, also aimed at preventing the commission of the Offenses contemplated in the Decree.

The adoption of the MOG enables Telepass to minimize the risk of criminal offenses being committed within the Company's structure to its advantage or in its interest.

Although the MOG is a legal instrument designed to protect the Company during criminal proceedings, it is important to emphasize that adherence to the MOG and its Control Measures by the Recipients helps prevent individuals from committing, either knowingly or unknowingly, unlawful acts during the performance of their work activities.

The MOG, therefore, serves as a protective tool for both the legal entity and the individuals who, in various capacities, operate within the corporate structure.

1. LEGISLATIVE DECREE NO. 231/2001

1.1 The Administrative Liability Regime for Entities

Legislative Decree No. 231/2001, titled *"Regulation of administrative liability of legal entities, companies, and associations, including those without legal personality"*, aligns Italian law on the administrative liability of legal entities and unincorporated associations ("Entities") with European conventions issued on the subject[1].

The Decree introduces a regime of liability that is formally administrative but substantively criminal in nature, applicable to Entities for certain Offenses committed in their interest or to their advantage by:

a) individuals in positions of representation, administration, or management of the Entity or its organizational units with financial and functional autonomy, as well as individuals who, even de facto, manage or control the Entity ("Top Management");

b) individuals subject to the direction or supervision of Top Management ("Subordinate Individuals").

The Entity's administrative liability is additional to the criminal liability of the natural person who materially committed the Offense. Both are ascertained within the same criminal proceeding before a penal judge. Moreover, the Entity's liability persists even if the natural person who committed the offense is not identified or is not legally culpable.

Currently, the Entity's liability arises exclusively in connection with the commission of the following predicate Offenses explicitly listed in the Decree:

i) Crimes against Public Administration (Articles 24 and 25, Legislative Decree 231/2001);

ii) Cybercrimes and unlawful data processing (Article 24-bis, Legislative Decree 231/2001);

iii) Organized crime offenses (Article 24-ter, Legislative Decree 231/2001);

iv) Forgery of money, public credit instruments, revenue stamps, and identification tools or signs (Article 25-bis, Legislative Decree 231/2001);

v) Crimes against industry and commerce (Article 25-bis.1, Legislative Decree 231/2001);

vi) Corporate crimes and private-to-private corruption (Article 25-ter, Legislative Decree 231/2001);

vii) Crimes for terrorism or subversion of democratic order (Article 25-quater, Legislative Decree 231/2001);

viii) Practices involving female genital mutilation (Article 25-quater.1, Legislative Decree 231/2001);

ix) Crimes against individual liberty (Article 25-quinquies, Legislative Decree 231/2001);

[1] The Brussels Convention of July 26, 1995 on the protection of the financial interests of the European Communities; the Brussels Convention of May 26, 1997 on cassombating corruption involving officials of the European Community or officials of Member States; the OECD Convention of December 17, 1997 on combating bribery of foreign public officials in international business transactions; the United Nations Convention and Protocols against Transnational Organized Crime, adopted by the General Assembly on November 15, 2000, and May 31, 2001, ratified in Italy by Law No. 146 of 2006.

x) Insider trading and market manipulation offenses (Article 25-sexies, Legislative Decree 231/2001);

xi) Negligent homicide or serious/very serious injuries due to workplace health and safety violations (Article 25-septies, Legislative Decree 231/2001);

xii) Receiving, laundering, and utilizing illicitly obtained money, goods, or benefits, as well as self-laundering (Article 25-octies, Legislative Decree 231/2001);

xiii) Offenses involving payment instruments other than cash and fraudulent transfer of assets or value (Article 25-octies.1, Legislative Decree 231/2001);

xiv) Copyright infringement crimes (Article 25-novies, Legislative Decree 231/2001);

xv) Inducing individuals to withhold statements or to provide false statements to judicial authorities (Article 25-decies, Legislative Decree 231/2001);

xvi) Environmental crimes (Article 25-undecies, Legislative Decree 231/2001);

xvii) Employment of third-country nationals whose stay is irregular (Article 25-duodecies, Legislative Decree 231/2001);

xviii) Hate crimes related to racism and xenophobia (Article 25-terdecies, Legislative Decree 231/2001);

xix) Fraud in sports competitions, unauthorized gambling, and illegal gaming operations via banned devices (Article 25-quaterdecies, Legislative Decree 231/2001)

xx) Tax crimes (Article 25-quinquiesdecies, Legislative Decree 231/2001);

xxi) Smuggling offenses (Article 25-sexiesdecies, Legislative Decree 231/2001);

xxii) Crimes against cultural heritage (Article 25-septiesdecies, Legislative Decree 231/2001);

xxiii) Laundering of cultural property and destruction or looting of cultural or landscape assets (Article 25-duodevicies, Legislative Decree 231/2001);

xxiv) Transnational crimes such as organized crime, money laundering, trafficking in migrants, and obstruction of justice (Law No. 146 of March 16, 2006, Articles 3 and 10);

xxv) Violations of the prohibitions imposed by EU Regulation 2023/1114 (the so-called MICAR Regulation concerning the provision of cryptocurrency services other than activities already regulated at EU level [2] (Legislative Decree No. 129/24).

Following an analysis of the Company's activities, it is believed that the offenses potentially relevant to Telepass include those under sub-paragraphs i), ii), iii), v), vi), vii), ix), x), xi), xii), xiii), xiv), xv), xvi), xvii), xx), xxi), and xxiv), provided they are committed in the interest or to the advantage of the Company pursuant to Article 5 of Legislative Decree 231/2001.

Offenses not considered potentially applicable to the Company have been excluded based on the nature of its activities and the absence of concrete risk scenarios.

[2] Technically, these offences are not included in the list of predicate offences, but Legislative Decree No. 129/24 refers to Decree 231 both with regard to the criteria for attribution and the applicable penalties. As a precautionary measure, therefore, they have been included in the list of offences that may result in the entity being held jointly liable.

The Control Measures – organizational and procedural – adopted by the Company are deemed adequate to prevent or minimize the risk of committing any of the offenses covered under Legislative Decree 231/2001.

1.2 **Offenses committed abroad**

An Entity can also be held liable for offenses committed abroad, provided that the Entity is not already being prosecuted by the state where the offense was committed. If the punishment of the perpetrator requires a formal request by the Minister of Justice, the Entity may be prosecuted only if such a request is also directed at the Entity. Specifically, pursuant to Article 4 of the Decree, an Entity with its principal office in Italy may be held accountable for offenses committed abroad if the following conditions are met:

a) the Offense was committed abroad by an individual functionally linked to the Entity (Article 5, paragraph 1, of the Decree);

b) the Entity has its principal place of business within Italian territory;

c) the Entity can be held accountable only in the cases and under the conditions provided for in Articles 7 (*Offenses committed abroad*), 8 (*Political offenses committed abroad*), 9 (*Common* offenses *committed abroad by an Italian citizen*), and 10 (*Common offenses committed abroad by a foreign citizen*) of the Italian Criminal Code.

Additionally, under Article 10 of Law No. 146/2006, an Entity can be held liable for certain transnational Offenses (such as the offense of criminal association, including mafia-type associations, the offense of association aimed at drug trafficking, and the offense of trafficking in migrants).

In such cases, the unlawful conduct, committed by an organized criminal group, must meet one of the following conditions:

i) be committed in multiple States;

ii) be committed in one state but have substantial effects in another State;

iii) be committed in one State, although a significant part of its preparation, planning, direction, or control takes place in another State;

iv) be committed in one State, involving an organized criminal group that engages in criminal activities across multiple States.

1.3 **Penalties**

The penalties provided for Offenses under the Decree are:

1) financial penalties;

2) prohibitory penalties;

3) confiscation;

4) publication of the ruling.

Financial penalties, applicable to all offenses, are determined based on a "quota" system. The judge establishes the number of quotas, taking into account the gravity of the act, the degree of the Entity's responsibility, and the actions taken to mitigate the consequences of the offense or prevent further offenses. The amount of each quota is set based on the Entity's economic and financial condition to ensure the penalty’s effectiveness (Article 11 of the Decree).

Prohibitory penalties can be applied to the Entity as a precautionary measure when there are serious indications suggesting its liability for the Offense, and when specific evidence indicates a tangible risk of similar offenses being committed (Article 45 of the Decree).

If a prohibitory penalty would result in the Entity's operations being interrupted, the judge may, instead of imposing the penalty, authorize the continuation of the Entity's activities under the management of a commissioner for a period equal to that of the prohibitory penalty. This is applicable if the Entity performs a public service or an essential service, where interruption would cause serious harm to the public, or if the interruption would have significant repercussions on employment.

Non-compliance with prohibitory penalties constitutes an independent offense under the Decree, potentially leading to further administrative liability for the Entity (Article 23 of the Decree).

Prohibitory penalties, lasting no less than three months and no more than two years, apply specifically to the activity related to the Offense and may include:

1) suspension of the business activity;
2) prohibition from contracting with Public Administration;
3) suspension or revocation of licenses, authorizations, or concessions related to the offense;
4) exclusion from public subsidies, contributions, or financing, or the revocation of those already granted;
5) prohibition from advertising goods or services.

Financial and prohibitory penalties are reduced by one-third to one-half when offenses under Articles 24 to 25-duodecies of the Decree are committed in the form of an attempt (Article 26 of the Decree).

In addition to the above penalties, the Decree mandates the **confiscation** of the price or proceeds of the offense, which may also include assets or other items of equivalent value, and the **publication of the ruling** when a prohibitory penalty is applied. The ruling is published in the municipality where the Entity's principal office is located and on the Ministry of Justice website.

It is worth noting that, in addition to the penalties provided under the Decree, the mere initiation of a criminal investigation for an administrative offense may result in a **reputational damage** to the Company and the Group, even if the proceedings result in dismissal or acquittal. Accordingly, all Recipients must strictly comply with the provisions of the MOG to avoid any involvement in criminal investigations.

1.4 Proceedings for Establishing the Offense and Evaluating the Adequacy of the Model by the Judge

Liability for an administrative offense arising from a predicate Offense is established within a criminal proceeding, which should remain combined – wherever possible – with the criminal proceeding against the individual who committed the predicate Offense for which the Entity is liable.

The determination of the Entity's liability, assigned to the criminal court, involves:

- verifying the existence of the predicate Offense;
- establishing whether the Entity benefited from or had an interest in the commission of the Offense;
- assessing the adequacy and effective implementation of the adopted Model.

The judge evaluates whether the Model is abstractly capable of preventing the Offenses covered under the Decree. This assessment is conducted retroactively, with the judge situating themselves within the corporate context as it existed at the time the offense occurred, to determine the effectiveness of the adopted Model in preventing the commission of the offense.

1.5 Adoption of the Model as a possible exemption from administrative liability

Articles 6 and 7 of the Decree provide specific conditions under which an Entity may be exempt from administrative liability for Offenses committed in its interest or to its advantage by either Top Management or Subordinate Individuals.

Specifically, Article 6 of the Decree stipulates that, in cases where Offenses are committed by Top Management, an Entity is exempt from administrative liability if it can demonstrate that:

a) the governing body adopted and effectively implemented, prior to the commission of the Offense, Models designed to prevent Offenses of the type that occurred;

b) the task of supervising the functioning of and compliance with the Models, as well as ensuring their updates, was assigned to a body with autonomous powers of initiative and control;

c) the individuals who committed the Offenses acted fraudulently to circumvent the Models;

d) there was no failure to supervise or insufficient supervision by the body referred to in letter b).

In the case of Offenses committed by Subordinate Individuals, Article 7 of the Decree states that the Entity is liable if the commission of the Offense was made possible by the failure to comply with management or supervision obligations. However, such failure is excluded if the Entity adopted and effectively implemented, prior to the Offense, a Model designed to prevent Offenses of the type in question.

The Decree further specifies that the Model must be adequate to address the following requirements:

1) identify the activities within which Offenses specified in the Decree could be committed;

2) provide specific protocols for planning and implementing the Entity’s decisions related to preventing such Offenses;

3) establish procedures for managing financial resources that prevent the commission of these Offenses;

4) impose obligations to inform the body responsible for overseeing the Model's implementation and compliance;

5) introduce an internal disciplinary system to sanction non-compliance with the measures outlined in the Model, including whistleblowing provisions as detailed later in the document.

2. THE COMPANY

Telepass is an Italian company operating in the field of urban and interurban mobility services based on apps, as defined below, aiming to create an ecosystem of services offering private individuals and companies an increasing number of flexible, secure, and sustainable integrated mobility options.

Specifically, Telepass engages in activities related to: (i) providing telepass services, enabling payment and seamless access to the toll motorway network through dedicated lanes without the need to stop at entry and exit toll stations; and (ii) providing additional services related to payment and/or facilitated access to areas, structures, infrastructures, and/or goods and services associated with mobility at facilities authorized to accept payments, including through its devices.

Furthermore, the Company's scope of activity has progressively expanded within the mobility services sector to include insurance brokerage, as a registered entity in Section E of the Single Register of Intermediaries (RUI) managed by IVASS. For the updated scope of activities, reference is made to the corporate purpose outlined in the Articles of Association approved at the Company's General Meeting on April 12, 2021.

Since 2016, the Company has been controlled by Mundys.

On April 14, 2021, 49% of Telepass's share capital was sold to the global investment manager Partners Group AG.

On May 1, 2022, Telepass Pay S.p.A., previously a subsidiary of Telepass, was merged into Telepass. Consequently, Telepass, authorized by the Bank of Italy, became an Electronic Money Institution (IMEL) through the establishment of a Dedicated Asset, as defined below, exclusively devoted to the issuance and distribution of electronic money and related services, as well as business functions dedicated solely to managing these activities (a "hybrid IMEL").

Based on the above, Telepass is authorized by the Bank of Italy to:

- issue and distribute electronic money;
- provide payment services unrelated to electronic money, as defined in Article 1, paragraph 2, letter h-septies.1), of Legislative Decree No. 385 of September 1, 1993, to offer new mobility-related services beyond those currently provided by Telepass under exemptions.

In the context of payment services operations, Telepass:

- issues and accepts payment instruments, specifically:
  - the physical device ("OBU");
  - the mobile application downloadable to smartphones ("App");
- executes payment orders, enabling its clients to initiate and complete payment operations through a website (accessible via computer or mobile web on smartphones), always ensuring strong customer authentication.

Telepass has either full or majority control over the following companies:

1) URBANnext S.A.;
2) Telepass Assicura S.r.l.;
3) Telepass Innova S.p.A.;
4) Eurotoll S.A.

Within the aforementioned activities, Telepass is subject to oversight by various administrative authorities, including, but not limited to, the Bank of Italy, the Italian Competition Authority (AGCM), IVASS, the Italian Data Protection Authority, and the Ministry of Infrastructure and Transport.

3. ADOPTION OF THE MODEL

3.1 Definition, objectives, and Recipients of this Model

The Model can be defined as a comprehensive set of principles, rules, provisions, organizational schemes, and related tasks and responsibilities, designed for the implementation and diligent management of a system for controlling and monitoring high-risk activities, with reference to the Offenses set forth in the Decree.

The **objectives** of this Model are as follows:

- to strengthen the corporate governance system;
- to establish a structured and systematic prevention and control system aimed at eliminating or reducing the risk of committing the Offenses under Legislative Decree 231/2001, including attempted offenses, related to the Company's activities, with particular attention to eliminating or reducing any illegal behaviours;
- to make all those who operate in the name, on behalf of, or in the interest of Telepass in high-Risk Areas aware that, in the event of a violation of the Model's provisions, they may incur a criminal or administrative offense, punishable not only against the individual author but also against the Company;
- to inform all those who operate in any capacity in the name, on behalf of, or in the interest of Telepass that violating the provisions contained in the Model will result in the application of appropriate sanctions;
- to emphasize that Telepass does not tolerate illegal behaviour, regardless of the pursued objective or the mistaken belief of acting in the Company's interest or for its benefit, as such behaviours are contrary to the ethical principles the Company aims to follow and, therefore, in contrast to its own interest;
- to address violations of the Model through the imposition of disciplinary and/or contractual sanctions.

The **Recipients** of this Model, who are required to be familiar with and comply with it within their specific competencies, are as follows:

- the members of the Board of Directors, responsible for setting objectives, deciding on activities, implementing projects, proposing investments, and making all decisions or actions related to the Company's operations;
- the members of the Board of Statutory Auditors, in the performance of their role of control and verification of the formal and substantial correctness of the Company's activities and the functioning of the internal control system;
- the CEO and the managers of the Company;
- employees and all collaborators with whom the Company maintains contractual relationships, in any capacity, including occasional and/or temporary relationships;
- all those who have commercial and/or financial relationships of any kind with the Company.

3.2 Structure of the Model adopted by Telepass

The Model adopted by Telepass consists of this General Section and the Special Sections prepared for the types of Offenses for which risks have been identified for the Company.

The Special Parts of this Model are divided into "Offense Families" that have been deemed relevant:

SPECIAL SECTION	OFFENCE FAMILY	DECREE
A	Offenses to the detriment of the Public Administration	Articles 24 and 25
B	Corporate crimes and corruption between private parties	Article 25-ter
C	Crimes and administrative offenses related to insider trading and market manipulation	Articles 25-sexies of the Decree and 187-quinquies TUF
D	Crimes of manslaughter or serious or very serious injury committed by violating health and safety at work regulations	Article 25-septies
E	Offenses of receiving, money laundering, and using money, goods, or benefits from illegal sources, as well as self-laundering	Law 231/2007 and Article 25-octies of the Decree
F	Computer crimes	Article 24-bis of the Decree and Law 48/2008
G	Environmental crimes	Article 25-undecies
H	Offenses involving the employment of citizens from third countries with irregular residency, and crimes against the individual's personality, particularly the crime under Article 603-bis of the Penal Code, "Illegal mediation and exploitation of labor"	Articles 25-duodecies and 25-quinquies
I	Crimes against industry and commerce and crimes related to copyright infringement	Articles 25-bis 1 and 25-novies
J	Tax crimes	Article 25-quinquiesdecies
K	Smuggling crimes	Article 25-sexiesdecies

L	Crimes committed with non-cash payment instruments and fraudulent transfer of assets or value	Article 25-octies.1
M	Crime of inducing false statements or withholding statements to the judicial authority	Article 25-decies
N	Criminal associations, both in the basic form under Article 416 of the Penal Code and in the transnational form under Law No. 146/2006 and offences relating to terrorism financing	Articles 24-ter, 25-quater and Law No. 146/2006

For all other offenses which, based on the analysis conducted, are deemed not to potentially concern the Company, and for which no specific Special Section has been prepared, the overall system of control, organizational, and procedural Control Measures adopted by the Company and referenced in this Model and in the Code of Ethics will apply.

3.3 **Update of the Model**

Given the complexity of the Company's organizational structure, to promote the compliance of the various business activities with the provisions of the Decree and, at the same time, ensure effective control over the risk of committing predicate Offenses, a continuous monitoring and updating process of the Model is foreseen in the event of one or more of the following conditions:

a. legislative and/or jurisprudential innovations regarding the liability of entities for administrative offenses resulting from crimes;

b. significant changes to the organizational structure and/or business sectors of the Company;

c. significant violations of the Model, results of the risk assessment, checks on the effectiveness of the Model, and industry best practices.

The Model is approved by the Board of Directors of Telepass.

After its initial issuance, the Model has been subject to updates based on the evolution of the regulatory and organizational framework.

Specifically:

i. in relation to the amendments introduced to the Decree by Law 62/2005 (the so-called Community Law 2004) and Law 262/2005 (the so-called Savings Law), Telepass updated the Model to account for the risks related to market manipulation and insider trading offenses, as well as the failure to communicate conflicts of interest;

ii. subsequently, in the 2010 update, the extensions of corporate liability were analyzed in relation to offenses of manslaughter and negligent injury due to violations of workplace health and safety regulations; offenses of receiving stolen goods, money laundering, and the use of money, goods, or benefits of illicit origin as provided by Article 25-octies; computer crimes and the unlawful processing of data; organized crime offenses; crimes against industry and commerce, and violations of copyright law; and, finally, offenses involving inducement not to make statements or to make false statements to the judicial authority;

iii. in **2013**, the Model was updated to account for the further expansion of predicate offenses, such as environmental crimes, the employment of third-country nationals with irregular residency, undue inducement to provide or promise benefits, and private corruption;

iv. in **2017**, the responsibility of entities was analysed further, in relation to the crime of self-laundering, environmental crimes under Law No. 68/2015, and provisions related to offenses against the individual, employment of third-country nationals with irregular residency, crimes against the public administration, mafia-type associations, and false accounting under Law No. 69/2015. Additionally, the 2017 update reflected the evolution of the Company's organizational structure;

v. in the **2019** update, the following legislative updates were incorporated:

   a. the crime of "incitement to private corruption" as per Legislative Decree 38/2017 (Article 25-ter of Legislative Decree 231/2001);

   b. amendments to the crime of "employing third-country nationals with irregular residency" as per Law 161/2017 (Article 25-duodecies of Legislative Decree 231/2001);

   c. introduction of the crime of "racism and xenophobia" under Law 167/2017 (Article 25-terdecies of Legislative Decree 231/2001), later amended by Legislative Decree 21/2018;

   d. introduction of "whistleblowing" provisions for the protection of those who report crimes or irregularities learned during public or private employment (Law 179/2017);

   e. amendments to environmental crimes (Article 25-undecies of Legislative Decree 231/2001) under Legislative Decree 21/2018;

   f. amendments to market abuse crimes (Article 25-sexies of Legislative Decree 231/2001) under Legislative Decree 107/2018;

   g. introduction of Law No. 3/2019 titled "Measures to combat crimes against public administration, prescription of crimes, and transparency of political parties and movements";

vi. in the **2021** update, the following were analysed and incorporated:

   a. new provisions regarding "tax crimes" introduced by the so-called Fiscal Decree converted into Law No. 157/2019 (Article 25-quinquiesdecies of Legislative Decree 231/2001);

   b. amendments to Articles 24, 25, and 25-quinquiesdecies of Legislative Decree 231/2001 and the inclusion of the crime of smuggling in the new Article 25-sexiesdecies, in implementation of the "PIF Directive" by Legislative Decree No. 75/2020[3];

   c. organizational and procedural changes affecting the Company;

vii. in the **2022** update, a comprehensive revision of the Model was carried out due to, among other factors:

   a. the merger between Telepass and its subsidiary Telepass Pay S.p.A., finalized on May 1, 2022, leading to the creation of a dedicated asset within Telepass for IMEL activities;

[3] Implementation of Directive (EU) 2017/1371, *"on the fight against fraud to the Union's financial interests by means of criminal law."*

b. internal reorganization of Telepass due to both the merger and the evolution of the Company's activities;

c. introduction of new potentially relevant predicate offenses for Telepass (i.e., crimes related to non-cash payment instruments, as per Legislative Decree No. 184/2021).

viii. in **2024**, the Model was updated due to the following factors:

a. amendments to the Whistleblowing regulation following the introduction of Legislative Decree No. 24/2023 and Telepass's adaptation to the new regulations;

b. introduction of new predicate offenses by Law No. 137/23, covering urgent measures regarding criminal and civil procedures, forest fire control, recovery from drug addiction, health, and culture;

c. transfer to the subsidiary K-Master S.r.l.[4] of the business unit owned by Telepass, consisting of the "Smart Device Unit" and the "R&D and Innovation Unit";

d. name change of the parent company from "Atlantia S.p.A." to "Mundys S.p.A.";

e. acquisition of a new subsidiary by Telepass;

f. update of the ISO certifications held by Telepass.

The 2024 update did not require a new risk assessment for the following reasons:

- regarding point a, a comprehensive review of the Model's reporting system was conducted, explicitly detailing protections under the new regulations and referring to the updated Whistleblowing Management Procedure. Specific guidelines were also introduced in the disciplinary system to sanction the failure to protect whistleblowers;
- regarding point b, the newly introduced offenses fall within risk areas already identified in previous versions of the Telepass Model, and the Company already has appropriate prevention protocols in place to address these new predicate Offenses;
- regarding point c, the Special Parts affected by the business unit transfer were reviewed based on a document analysis (deed of transfer, existing service contracts between Telepass and its subsidiary) and in consultation with the relevant departments of Telepass or Telepass Innova S.p.A.;
- regarding points d, e, and f, changes were mainly nominal in nature.

ix. in **2025** a number of updates were made to the Model mainly due to the following factors:

a. the introduction of new predicate offences, as well as the amendments and repeal of other predicate offences (e.g. in the area of offences against the Public Administration, cybercrimes, etc.);

b. changes in the list of companies controlled by Telepass.

The 2025 update did not require a new corporate risk assessment, as the changes to the predicate offences affect areas of activity already covered in previous revisions of the Model.

In all cases where regulatory or corporate changes require a reassessment of corporate risks, the Company shall proceed as described below.

[4] Subsequently merged into Infoblu S.p.A., which later changed its name to Telepass Innova S.p.A.

3.3.1 Mapping of activities at risk of Offenses

First, the Company evaluates business activities, organizational areas, and processes where predicate offenses could theoretically be committed in the interest or for the benefit of the Company, as well as activities that could facilitate or contribute to the commission of such offenses.

The identification of at-risk processes/activities is carried out by examining corporate documentation (e.g., organizational charts, key processes, powers of attorney, organizational directives), analysing the Company's critical processes, and conducting a series of interviews with key individuals involved in at-risk processes/activities.

Among the Risk Areas, the Company includes not only those activities **directly** linked to the potential commission of Offenses but also those that may **indirectly**/**instrumentally** contribute to their commission. Instrumental activities, in particular, are those that can create the factual conditions necessary to commit Offenses.

3.3.2 Risk Assessment

The information gathered through interviews and the analysis of documentation provides the necessary elements to perform a risk assessment.

For each identified Risk Area, the Company evaluates the likelihood of each specific predicate Offense contemplated under the Decree being committed.

3.3.3 Control Measures adopted by Telepass

Once potential risks are identified, the Company analyses the system of Control Measures within the at-risk processes/activities to assess their adequacy in preventing the identified risks of Offenses.

During this phase, the existing Control Measures are examined (e.g., formal procedures, adopted practices, traceability and documentation of operations and controls, segregation of duties) by analysing the information and documentation provided by corporate structures.

In the context of the risk assessment, the following components of the preventive control system are analysed:

1) delegation and power of attorney system;
2) organizational system;
3) management control and financial flow system;
4) control measures;
5) integrated control system.

The checks on the control system also encompass activities conducted with the support of Telepass Group companies or external providers (outsourcing).

These checks are based on the following criteria:

- the formalization of services provided in specific service contracts;
- the inclusion of adequate control measures for activities carried out by service companies based on the contractually defined services;
- the existence of formalized procedures/guidelines for drafting service contracts and implementing control measures, including criteria for determining fees and payment authorization procedures.

Delegation and Power of Attorney System

Telepass adopts a traditional administration and control model, where:

- the Board of Directors exercises strategic oversight functions;
- the CEO exercises management functions;
- the Board of Statutory Auditors exercises supervisory functions as defined in the Articles of Association, while the auditing of accounts is entrusted to an external audit firm.

The Board of Directors has established, in accordance with Article 42 of the Articles of Association approved at the General Meeting on April 12, 2021, the following Board Committees:

- Human Resources and Remuneration Committee;
- Control, Risk, and Sustainability Committee;
- Technology and Innovation Committee.

As recommended by corporate best practices and specified in the Confindustria Guidelines, the Telepass Board of Directors assigns and revokes powers to the Chairman, the CEO, and any Directors entrusted with specific delegations, defining their scope and content.

The Board of Directors formally grants powers to the Chairman, CEO, and, when necessary, managers, up to a defined expenditure threshold. Beyond this threshold, prior approval from the Board of Directors is required, along with the issuance of the corresponding mandate.

The Chairman and the CEO, within the powers conferred by the Board of Directors and in line with defined organizational and managerial responsibilities, delegate operational powers to managers, employees, and third parties, specifying clear expenditure thresholds.

The level of autonomy, representation authority, and spending limits assigned to individuals holding delegations and powers of attorney within the Company are established in strict compliance with the hierarchical level of the recipient. These powers are updated based on organizational changes within the Company's structure.

In matters of health and safety in the workplace, the Board of Directors has assigned the role of Employer to the Chief People and Organization Officer.

Following its designation as **hybrid IMEL** on May 1, 2022, Telepass established a dedicated asset related to electronic money and payment services (the"Dedicated Asset"), corresponding to the activities and services previously managed by its subsidiary Telepass Pay S.p.A. (merged into Telepass). Specifically:

i) the assets and legal relationships assigned to the Dedicated Asset are exclusively intended to fulfill the rights of payment service users, constituting a separate asset from Telepass's residual general assets (the "Free Asset");

ii) in the event of insufficiency of the Dedicated Asset, Telepass is also liable with its general assets for obligations towards payment service users and other parties holding rights arising from the exercise of related and ancillary activities;

iii) Telepass must keep, for the Dedicated Asset, separate books and accounting records as prescribed by Articles 2214 *et seq.* of the Italian Civil Code, in compliance with international accounting standards. Specifically, Telepass's Directors must prepare a separate financial statement for the Dedicated Asset, to be attached to the Company's annual financial statements.

iv) The financial statement of the Dedicated Asset must be accompanied by a specific report prepared by the entity responsible for the statutory audit, certifying the consistency of the data contained therein with those reported in Telepass's financial statements.

v) On May 28, 2021, the Board of Directors of Telepass appointed a General Manager and Dedicated Asset Manager, tasked with overseeing the functions and activities related to the hybrid IMEL operations.

The General Manager, as the Dedicated Asset Manager, is tasked, in summary, with the following responsibilities:

i) ensuring, in coordination with the corporate bodies, that the Company's organizational structure is adequate to its size, complexity, and operations. To this end, the General Manager is entrusted with, by way of example and not limitation, the following responsibilities:

   a. defining, in collaboration with the CEO, information flows to ensure that corporate bodies are fully informed of significant management matters;

   b. defining the duties and responsibilities of the corporate structures under their supervision, with the aim, among other things, of preventing potential conflicts of interest and ensuring that such structures are led by personnel qualified for the activities to be performed;

   c. establishing and implementing the Company's policy regarding the outsourcing of corporate functions;

   d. ensuring, in collaboration with the CEO, that personnel and agents engaged in the provision of payment services, as well as personnel and parties contracted for the distribution and redemption of electronic money, are adequately trained on the marketed products and provided services, compliance with anti-money laundering and counter-terrorism financing regulations, and transparency requirements.

ii) defining governance and control procedures for products as required by transparency regulations;

iii) with reference to the provision of payment services and the issuance of electronic money, strategic decisions regarding entry into new sectors and/or the introduction of new products and/or services are made by the Board of Directors, based on proposals submitted by the CEO, and following consultation and approval by the General Manager for regulatory matters;

iv) establishing the General Anti-Money Laundering Procedure ("AML Policy"), taking into account the guidance and recommendations provided by competent authorities and various international bodies, as well as developments in the regulatory framework, and defining internal management and control procedures within the scope of anti-money laundering regulations.

Organizational system

The internal organizational structure of the Company is represented:

- at the macro level, through an organizational chart specifying:
  - the structures into which the Company's activities are divided at the first hierarchical level, including the names of the managers responsible for each structure;
  - the lines of hierarchical dependency.
- at the micro level, by specifying for each structure:
  - the organizational breakdown, including the name of the manager and the hierarchical dependencies;
  - the resources operating in each area, their employment level, and their organizational position.

Documents related to the internal organizational structure are periodically updated by the People and Organization department.

In matters of health and safety at work, the Company, in line with the current organizational structure and the powers assigned to the Employer, identifies the roles and responsibilities required under Legislative Decree No. 81/2008.

As part of the Model updating process, the adequacy of the organizational system has been assessed based on the following criteria:

- formalization of the system;
- clear definition of responsibilities and hierarchical dependencies;
- existence of segregation and checks between functions;
- consistency between the activities actually carried out and the missions and responsibilities described in the Company's organizational chart.

Some organizational structures are exclusively dedicated to the operation of the Dedicated Asset, including:

- the **Anti-Money Laundering Officer and Suspicious Activity Delegate**, responsible for preventing and combating money laundering and terrorist financing activities;
- the **Outsourced Activities Referent** ("RAE"), reporting directly to the General Manager. While the Board of Directors and the CEO retain decision-making authority on outsourcing business functions, the RAE manages and supervises risks related to outsourcing agreements within the internal control system.

To ensure compliance with regulatory requirements regarding administrative and accounting organization, as well as internal controls, the following safeguards have been implemented:

- the Board of Directors is supported in its responsibilities by internal committees – particularly the Control, Risk, and Sustainability Committee – which has preparatory and advisory functions regarding any regulatory issues related to the provision of payment services and electronic money, and therefore the operation of the Dedicated Asset.
- an adequate internal control system has been established to monitor compliance with the requirements set by the supervisory Authorities.

In addition, for both activities related to the Dedicated Asset and non-regulated activities, the following functions and entities serve as safeguards:

- **Data Protection Officer** ("DPO"), responsible for monitoring regulatory developments in data privacy, providing information and advice on data protection obligations, verifying compliance with regulations and internal policies, and offering, when requested, opinions on data protection impact assessments. The DPO also serves as the point of contact with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali).
- **Chief Information Security Officer** ("CISO"), responsible for monitoring IT security systems, developing, and implementing processes to mitigate cybersecurity risks.
- **Ethics Officer**, who reports to the Board of Directors and the CEO; responsible for monitoring compliance with the Code of Ethics, serving as a point of contact for Telepass employees and those of its subsidiaries for ethical concerns, and supporting the Company in planning initiatives to foster a strong ethical culture.
- **Whistleblowing Team**, whose roles and responsibilities are described in Section 5.5.

Management control system and financial flows

The operational management control system of Telepass is based on the following control principles:

- definition, on an annual basis, of the resources (both financial and non-financial) allocated to each company structure, along with the scope within which these resources can be used, through the programming and definition of the budget;
- monitoring/ analysis of variations from the budgeted amounts, examining the causes and reporting the results of these assessments to the appropriate hierarchical levels for the necessary corrective actions, through the corresponding final account statements;
- monitoring of the compliance of the authorization process in accordance with the internal delegation and power of attorney system.

The management of financial resources is based on principles of segregation of duties, ensuring that all expenses are requested, executed, and controlled by distinct individuals.

The management of liquidity follows principles aimed at the preservation of assets, with a related prohibition on performing high-risk financial transactions.

Additionally, Telepass utilizes a system of legal auditing of accounts.

Control Measures

The Company has developed a set of procedures aimed at regulating the structure of the business processes that make up the organization. These procedures describe the methods of carrying out activities, identify the contents and responsibilities, and outline the control and monitoring activities to be performed in order to ensure the correctness, effectiveness, and efficiency of the corporate activities that are of particular importance, as well as to define the correct management procedures to follow.

In the Special Sections of this Model, the procedures, policies, guidelines, and protocols, regardless of their designation, implemented by Telepass will be referenced as appropriate.

Furthermore, the Company has obtained the following certifications:

1) ISO 45001:2018, Occupational Health and Safety Management System;

2) ISO 27001:2022, Information Security Management System;

3) ISO 14001:2015, Environmental Management System;

4) ISO 9001:2015, Quality Management System.

The evaluation of the adequacy of the Control Measures, in the process of updating the Model, has taken into account not only the negotiation phases but also those related to the instruction and training of corporate decisions.

In particular, with regard to the activities of IMEL, Telepass has implemented a set of procedures designed to prevent the risk of money laundering and financing of terrorism, which are outlined in the relevant Special Sections.

Integrated control system

Telepass' integrated control system is structured, as recommended by best practices in the field, into three levels:

- 1st level: also referred to as "line control", it involves the control directly exercised by the managers of operational areas who are responsible for risk management and the implementation of Control Measures;
- 2nd level: this control is exercised by the corporate functions responsible for monitoring and managing typical risks.
- 3rd level: this control is performed by the Internal Audit function of the Telepass Group.

With respect to **2nd level controls**, Telepass has adopted a control system consisting of two functions:

1) Risk Management Function;

2) Compliance & AML Financial Services Function.

Within the **Risk Management** function, the Risk Officer is tasked with contributing to the definition of methodologies for measuring business risks, verifying compliance with the limits assigned to various operational areas, and ensuring the consistency of operations with the risk appetite objectives assigned.

The head of the **Compliance & AML Financial Services** function reports functionally to the General Manager and the Head of the Designated Assets, and hierarchically to the CEO. This function is responsible for assessing the adequacy of internal procedures with respect to the objective of preventing violations of mandatory laws and regulations, as well as self-regulation (statutes, codes of conduct, self-discipline codes) applicable to Telepass.

3rd level controls involve periodic oversight carried out by the **Internal Audit** function, which reports directly to the Board of Directors, ensuring that its head is not hierarchically subordinate to the heads of the functions under review. This function adheres to international methodological standards for the professional practice of internal auditing: the International Professional Practices Framework ("IPPF"). Within 3rd level control, Internal Audit identifies and assesses the adequacy and effectiveness of the adopted Internal Control and Risk Management System (*Sistema di Controllo Interno e Gestione dei Rischi*, "SCIGR") applied to the processes and activities under analysis, evaluating the evidence collected with independence, professionalism, integrity, objectivity, confidentiality, and competence. Additionally, Internal Audit assesses necessary updates to the Audit

Plan for emerging risks and considers, for "extra-plan" interventions, input received not only from the corporate bodies but also from the Supervisory Body.

Furthermore, the **Anti-Corruption Officer** ensures continuous monitoring of the risk of corruption and periodically reports on their activities to the Company's Supervisory Body, ensuring coordination with the same Body for the effective performance of their respective duties, as well as to the Board of Directors and the CEO.

Regarding **health and safety at work**, within the aforementioned integrated management system, the Company has also adopted and formally implemented a monitoring system for compliance with health and safety obligations, which directly reports to the Employers (for details, see the Special Section D).

The analysis of the integrated control system in the process of updating the Model addressed the existence of an adequate monitoring system for process verification, including the results and any non-conformities, as well as an appropriate documentation management system ensuring traceability of operations.

Gap Analysis

The design of the identified controls is then compared with the characteristics and objectives required by the Decree and/or suggested by the Confindustria Guidelines and best national and international practices.

The overall assessment of the adequacy of the control system is carried out taking into account the acceptable level of risk, which is approved by the Board of Directors from time to time.

3.4 Adoption of a "231" compliance model or mechanisms by Telepass subsidiaries

Each company within the Telepass Group, as an individual subject to the provisions of Legislative Decree No. 231/2001, must evaluate the appropriateness of adopting and periodically reviewing its own Organizational, Management, and Control Model or implementing "231" compliance mechanisms tailored to its specific characteristics (in terms of size, organization, business, etc.), thereby confirming the autonomy of each subsidiary within the Group.

Only the individual subsidiary can perform a precise and effective assessment and management of the risks associated with the potential commission of offenses, which is necessary for the Model to be recognized as having the exempting effectiveness described in Article 6 of the Decree.

A subsidiary that adopts its own Model, tailored to its specific context, must establish an independent and autonomous Supervisory Body, primarily responsible for overseeing the implementation of the Model according to the procedures described therein and in compliance with Articles 6 and 7 of the Decree.

The Telepass Model serves as a reference for defining the organizational models of its subsidiaries, particularly with regard to the principles outlined therein.

Each subsidiary must identify its own sensitive activities and specific protocols based on the peculiarities of its corporate reality. Additionally, any amendments or updates to the Telepass Model must be promptly communicated to the subsidiaries so that, within their autonomy, they can evaluate the potential need to update their respective Organizational, Management, and Control Models or the adopted compliance mechanisms.

3.5 Communication of the Model

Telepass promotes awareness of the Model, the internal regulatory framework, and relevant updates among all Recipients, with varying levels of detail depending on their position and role.

Recipients are therefore required to familiarize themselves with the content of the Model, adhere to its provisions, and contribute to its implementation, including through mandatory training on "231" compliance.

For employees, the Model is made available on the digital intranet platform “T-Space”, which they can access during their routine work activities.

Upon hiring, employees also receive an Information notice on corporate provisions, which includes, among other things, a reference to the Model and relevant regulations pertinent to the Company, whose knowledge is necessary for the proper performance of work activities.

The General Section of this Model and the Code of Ethics are made available to third parties and any other stakeholders of the Company required to comply with its provisions, through publication on the Company’s website.

4. SUPERVISORY BODY

4.1 Identification of the Supervisory Body

In compliance with the Decree and the Confindustria Guidelines, the Board of Directors of Telepass has established a body (the "Supervisory Body" or "SB") tasked with overseeing the functioning, effectiveness, and compliance of the Model, as well as ensuring its updates.

Given the specificity of its duties, the Supervisory Body is composed of multiple members, including at least one external member who acts as the Coordinator. Other members of the Supervisory Body are selected from both external and internal individuals within the Company who, in the course of their duties, are not subject to the hierarchical authority of any corporate body or function.

4.2 Appointment

The members of the Supervisory Body are appointed by the Board of Directors, which also identifies the Coordinator. The appointment is communicated to each member of the Supervisory Body through the Company's Board resolution communication system. Each member must formally accept the appointment.

The composition, duties, prerogatives, and responsibilities of the Supervisory Body, as well as the purpose of its establishment, are communicated across all corporate levels.

4.3 Requirements of the Supervisory Body

Pursuant to Articles 6 and 7 of the Decree and considering the Confindustria Guidelines, the Supervisory Body must consistently ensure its autonomy and independence, professionalism, and continuity of action.

The autonomy and independence are guaranteed through the presence of a respected external member serving as Coordinator, free of operational duties or interests that could impair their independent judgment. Additionally, the Supervisory Body operates without hierarchical constraints within the corporate governance framework, reporting directly to the Board of Directors, the Board of Statutory Auditors, and the Chairman and CEO.

When selecting the members of the Supervisory Body (SB), the Board of Directors considers specific skills and professional experience in legal fields – particularly in the prevention of offenses under Legislative Decree No. 231/2001 and criminal law – as well as in corporate management and organization, to ensure the Body's professionalism.

Furthermore, given the unique nature of the tasks and the specific professional expertise required for the assigned duties, the Telepass Supervisory Body utilizes the support of other structures within the Company or the Telepass Group and/or external consultants as needed.

The continuity of action is ensured by the fact that the Supervisory Body operates within the Company and that its members possess in-depth and comprehensive knowledge of corporate processes, enabling them to promptly identify any critical issues.

The appointment as a member of the Supervisory Body is conditional upon the absence of incompatibility and the possession of good standing. Causes of ineligibility or disqualification include:

- being a Director of Telepass or its subsidiaries;
- having close familial relationships (up to the fourth degree) with Directors of Telepass;

- maintaining, directly or indirectly (excluding an existing permanent employment relationship), economic relationships and/or contractual agreements, whether for consideration or free of charge, with Telepass and/or its Directors that are significant enough to impair independent judgment;
- holding, directly or indirectly, shareholdings in Telepass that enable control or significant influence over the Company or otherwise compromise independence;
- holding delegations, powers of attorney, or, more generally, roles or responsibilities that could undermine independent judgment.

With regard to the good standing requirements that members of the Supervisory Body must meet, the following constitute grounds for ineligibility and incompatibility for holding the position: being under indictment for an intentional crime or being subject to a personal precautionary measure.

4.4 Term and revocation

The Board of Directors determines the term of office for Supervisory Body members. Each member serves until their successor is appointed or a new Supervisory Body is formed.

The Board of Directors, after consulting the Board of Statutory Auditors, has exclusive authority to revoke the Supervisory Body or its members at any time for just cause, which includes: a) disqualification, interdiction, or a serious illness rendering the member unable to perform their supervisory duties; b) assignment of operational functions and responsibilities to the member that are incompatible with the Supervisory Body's requirements for autonomy, independence, and continuity of action; c) serious breach of the duties of the Supervisory Body as defined in the Model; d) breach of the obligation of confidentiality; e) loss of good standing requirements.

In cases of revocation of all members, the Board of Directors, after consulting the Board of Statutory Auditors, must establish a new Supervisory Body.

In the presence of serious reasons, the Board of Directors, after consulting the Board of Statutory Auditors and, if not involved, the other members of the Supervisory Body, will arrange for the suspension of one or all members of the Supervisory Body and promptly appoint a new member or an entirely new Supervisory Body.

4.5 Functions and powers of the Supervisory Body

The Supervisory Body of Telepass is entrusted with the following general duties:

a) to monitor the adequacy of the Model in preventing the commission of the Offences referred to in the Decree;

b) to oversee compliance with the provisions of the Model by internal Recipients of the Company and to promote the same compliance by Third-Party Recipients (consultants, suppliers, etc.);

c) to ensure the updating of the Model in relation to changes in the organizational structure, the regulatory framework, or as a result of the monitoring activities following which significant violations of the provisions are discovered.

On a more operational level, the Supervisory Body of Telepass is tasked with:

- constantly carrying out a review of the company's activities and the applicable regulations, for the purpose of updating the Company's mapping of activities at risk of criminal offences and proposing the update and integration of the Model and procedures, where necessary;

- monitoring the ongoing validity of the Model and procedures and their effective implementation, promoting, also after consulting the relevant company departments, all necessary actions to ensure their effectiveness. This task includes the formulation of proposals for adjustments and subsequent verification of the implementation and functionality of the proposed solutions;
- periodically conducting targeted checks on specific transactions or acts carried out within high-risk activities;
- verifying the existing authorization and signing powers, in order to assess their consistency with the defined organizational and management responsibilities, and proposing their update and/or modification when necessary;
- defining and managing, in accordance with the Model, the periodic information flow, with a frequency appropriate to the criminal risk level of each area, to allow the Supervisory Body to be regularly updated by the relevant departments on activities assessed as being at risk of criminal offences, as well as establishing communication procedures to gather information on potential violations of the Model;
- implementing, in compliance with the Model, a periodic information flow to the relevant corporate bodies regarding the effectiveness and compliance with the Model;
- sharing the training programs promoted by the Company to spread knowledge and understanding of the Model;
- verifying the initiatives taken by the Company to facilitate the knowledge and understanding of the Model and its related procedures by all those who act on behalf of the Company;
- verifying the credibility of reports received regarding behaviors considered to constitute criminal offenses under the Decree;
- investigating the causes that led to the alleged violation of the Model and identifying the individuals responsible for it;
- verifying reported or discovered violations of the Model and ensuring that they are communicated to the relevant departments for disciplinary purposes.

For the performance of its duties, the Supervisory Body is vested with the following powers:

- to access any relevant company document and/or information necessary for the performance of the functions assigned to the Supervisory Body under the Model. All company functions, employees, and members of the corporate bodies are required to provide any information in their possession upon request by the Supervisory Body or when relevant events or circumstances arise for the execution of the Body's activities;
- to access, without the need for prior consent, any company structure in order to obtain any information or data deemed necessary for the performance of its duties;
- to engage external consultants with proven expertise where necessary for the execution of its tasks;
- to ensure that the heads of company departments provide the requested information, data, and/or reports in a timely manner;

- to request, if necessary, the direct hearing of employees, Directors, and members of the Board of Statutory Auditors of the Company;
- to request information from external consultants, commercial partners, and auditors.

In order to better and more effectively carry out the duties and functions assigned to it, the Supervisory Body may avail itself, to support its operational activities, of the Telepass Group Internal Audit Function, in coordination with the latter, as well as other company departments, which may prove useful from time to time in the performance of the indicated activities.

To guarantee its independence, the Supervisory Body reports directly to the Board of Directors and, in performing its functions, operates with full autonomy, having adequate financial resources to ensure its total operational independence.

To this end, the Board of Directors allocates to the Supervisory Body the financial resources it deems necessary for the expenses incurred in the performance of its duties.

In the execution of the operational activities delegated by the Supervisory Body, the departments in charge report solely to the Supervisory Body on their activities, and similarly, the Supervisory Body reports to the Board of Directors on the activities carried out on its behalf by company departments and external consultants.

4.6 **Reporting to corporate bodies**

The Supervisory Body reports annually on its activities to the Board of Directors and the Board of Statutory Auditors, without prejudice to the specific need for the Supervisory Body to provide reports or communicate with the Board of Directors, the Board of Statutory Auditors, or other corporate bodies at other times. In particular, the report shall cover the following:

- the overall activities carried out during the period, with particular reference to the monitoring of the adequacy and actual implementation of the Model;
- any issues that have arisen, both in terms of internal behaviors or events within the Company, that may lead to violations of the Model's provisions;
- corrective and improvement actions proposed for the Model and their implementation status;
- any reports received during the year and the actions taken by the Supervisory Body and other relevant parties;
- any other information deemed useful for the purpose.

The Supervisory Body must also report promptly to the Chairman and the Chief Executive Officer regarding:

- any violation of the Model deemed well-founded, of which it has become aware either through reports from employees or following direct investigations by the Supervisory Body;
- identified organizational or procedural deficiencies that may create a tangible risk of the commission of offences relevant under the Decree;
- particularly significant regulatory changes that affect the implementation and effectiveness of the Model;
- lack of cooperation from company departments;

- any other information deemed useful for urgent decisions to be made by the Chairman and the Chief Executive Officer.

4.7 Operating Regulations

The Supervisory Body adopts and approves internal regulations governing its operations ("Supervisory Body Regulations").

4.8 Relationships with upervisory Bodies of Telepass Group companies

In compliance with the mutual autonomy and confidentiality of the information pertaining to the various companies within the Telepass Group, the Supervisory Body may communicate with the Supervisory Bodies, where present, of the subsidiary companies for the effective implementation of their respective models.

The communication flows may cover the methods of activity planning, the initiatives undertaken, any violations of the Model, sanctions imposed, and issues identified during the monitoring activities, in order to identify and understand areas of activity that have been found to be at risk.

4.9 Relationships with the Board of Statutory Auditors

In respect of mutual autonomy, the Supervisory Body shall inform the Board of Statutory Auditors, at its request, regarding the compliance with and updating of the Model.

5. INFORMATION FLOWS TO THE SUPERVISORY BODY

5.1 Information flows from Company departments

The obligation to establish a structured information flow is one of the tools to ensure the Supervisory Body's monitoring of the adequacy and effectiveness of the Model and for the possible retrospective investigation of the causes that enabled the commission of offences covered by the Decree.

The Supervisory Body must be made aware of all relevant information, in addition to that specified in the Special Sections of the Model and company procedures, including any information from third parties related to the implementation of the Model in "at-risk" activities.

In particular, the company's organizational structures, each within their area of responsibility, are required to report to the Supervisory Body any information regarding:

- the commission of crimes or the performance of acts that may result in their commission;
- the commission of administrative offences;
- behaviours not in line with the conduct rules set out in this Model and related protocols;
- any changes in the company's organizational structure or procedures;
- any changes to the delegation and proxy system;
- operations of particular importance or that present such levels of risk that they raise a reasonable concern about the potential commission of crimes;
- measures and/or information from law enforcement agencies or any other authority indicating that investigations are being carried out against Telepass employees or collaborators in the course of their work functions for Telepass or its subsidiaries;
- requests for legal assistance submitted by executives and/or employees in the event of the initiation of criminal proceedings[5];
- reports prepared by the heads of company departments within their control activities, from which possible violations of the Model's rules emerge;
- information regarding the actual implementation of the Model at all levels of the company, including details of any disciplinary proceedings conducted, any sanctions imposed, or any decisions to close such proceedings, with related justifications;
- initiation of inspection actions by public bodies (e.g., judiciary, the Italian finance police (*Guardia di Finanza*), other Authorities, etc.) within the scope of high-risk activities.

Other information flows to be transmitted to the Supervisory Body are referred to in the specific procedure dedicated to them.

As further specified in the Whistleblowing Management Procedure and section 5.4 of this Model, reports regarding alleged violations of the Model can also be submitted directly to the Supervisory Body.

The Supervisory Body shall act in a manner that guarantees whistleblowers protection from any form of retaliation, discrimination, or penalization, and also ensures the confidentiality of the

[5] See the Guidelines "Code of Conduct regarding the management of legal representation for employees and executives involved in judicial proceedings" dated 01/04/2021.

whistleblower's identity, in accordance with the legislation on whistleblowing, the Whistleblowing Management Procedure, and the guidelines of the Organizational Model.

To facilitate the direct submission of reports to the Supervisory Body, the Company has established dedicated communication channels:

- email address: organismodivigilanza@telepass.it;
- ordinary mail at the address: Organismo di Vigilanza, Telepass S.p.A., Via Laurentina n. 449 – 00142 Rome, Italy.

The management of reports is carried out according to the procedures described in section 5.4 of this Model, to which full reference is made.

5.2 Reporting obligations regarding official acts

In addition to the information mentioned in the previous section, the following information must be compulsorily transmitted to the Supervisory Body of Telepass:

- measures and/or information from law enforcement agencies or any other authority indicating that investigations, even against unknown individuals, are being carried out for offences under the Decree attributable to the Company;
- requests for legal assistance submitted by executives and/or employees in the event of the initiation of judicial proceedings for offences under the Decree attributable to the Company;
- reports prepared by the heads of company departments within their control activities, from which facts, acts, events, or omissions with critical profiles regarding compliance with the provisions of the Decree may emerge;
- information regarding the actual implementation of the organizational Model at all company levels, including details of any disciplinary proceedings conducted and any sanctions imposed (including measures against employees), or any decisions to close such proceedings, with related justifications.

5.3 Collection, storage, and access to the Supervisory Body's archive

All documentation related to the information flows received must be stored under the responsibility of the Secretary of the Supervisory Body.

5.4 Whistleblowing

Whistleblowing is a legal concept originating from European Union law aimed at preventing unlawful activities in both public and private organizations and protecting individuals who report illegal activities or fraudulent actions within the organization (public or private) to which they belong.

This concept had already been regulated for the private sector by Legislative Decree 231/2001 (Article 6, paragraphs 2-bis, 2-ter, 2-quater).

With Legislative Decree no. 24/2023 – the regulatory instrument implementing European Directive 2019/1937 on the protection of whistleblowers – the adoption of a whistleblowing system became mandatory for certain types of companies operating in the private sector, and the operational management of reporting procedures was regulated.

The National Anti-Corruption Authority subsequently issued specific Guidelines containing detailed rules for establishing suitable channels for managing reports[6], to which Telepass has adhered.

To comply with the new regulations, Telepass, which had already implemented a whistleblowing management system under previous regulations, has updated its Whistleblowing Management Procedure, applicable to all Telepass Group companies.

This procedure governs:

- the process for receiving, analyzing, and handling reports;
- the procedures for managing the related investigations, in compliance with privacy laws and/or other applicable laws in the country where the reported event occurred, applicable to the individual and subject of the report;
- the protections provided to the whistleblower and other individuals identified by law;
- the content of reports;
- the roles, responsibilities, and areas of application.

Telepass, to facilitate the submission of reports, has established the following official channels:

- email address: segnalazioni.telepass@telepass.com;
- physical mail: Telepass S.p.A., Segnalazioni Team (*Reporting Team*), Via Laurentina, 449 - 00142 Rome;
- online platform, accessible by all whistleblowers (employees, third parties, etc.) on the Telepass website.

Oral reports may be made via suitable channels (e.g., voicemail) or through a direct meeting with the Reporting Team or one or more of its members, at the request of the whistleblower.

The digital platform does not replace other reporting channels but expands the possibilities for submitting a report. It allows anyone (employees, collaborators, suppliers, or any other individual who has had or intends to establish business relations with the Telepass Group companies) to report suspected illegal conduct or irregularities, violations of rules, violations of the Model, violations of the Code of Ethics, violations of the Anti-Corruption Policy, and violations of corporate procedures and regulations in general.

In particular, the whistleblower, while required to register on the platform, has the option to make anonymous reports, as their access credentials, if present, are securely stored, protected, and accessible only by the third-party platform manager and are not associated with the report submitted to Telepass.

If the whistleblower prefers, they may provide their name in the report, explicitly consenting to the disclosure of their identity to the Reporting Team.

For reports sent via physical mail and email channels, the confidentiality of the whistleblower's identity (as well as the content of the report) is protected as follows:

[6] Guidelines on the Protection of Persons Reporting Violations of Union Law and the Protection of Persons Reporting Violations of National Regulatory Provisions. Procedures for the Submission and Management of External Reports, 12 July 2023.

- physical mail addressed to the Reporting Team is delivered in a sealed envelope (as delivered by the postal service) to the Technical Secretariat of the Reporting Team;
- the email inbox is accessible only by members of the Reporting Team and the Technical Secretariat; the administrator of the corporate email system may access the inbox only for technical needs, upon written request on a case-by-case basis submitted to the Reporting Team Coordinator, and access will be granted only with prior written authorization from the Reporting Team Coordinator.

In cases where the whistleblower's name has been disclosed, the whistleblower's identity is separated from the content of the report during the handling process, and replaced by an alphanumeric code assigned to the whistleblower during the initial registration in the dedicated Register kept by the Technical Secretariat.

If the allegation is founded, in whole or in part, and knowledge of the whistleblower's identity is essential for the defence of the accused individual, the report may only be used for disciplinary proceedings if the whistleblower has explicitly consented to the disclosure of their identity. The whistleblower will be notified in writing of the reasons for disclosing their confidential data, as required by law.

In the following cases, however, there is no legal obligation to protect the confidentiality of the whistleblower's identity:

- the report is found to be false and made with the intent to harm or damage the reported party (so-called "bad faith reporting"), and constitutes criminal defamation or slander under the law;
- the report reveals facts and/or circumstances that, although unrelated to the company sphere, make it appropriate and/or necessary to report the matter to the judicial authority (e.g., terrorism or espionage offenses).

The body responsible for managing the process of evaluating reports is the **Reporting Team**, which carries out its functions for Telepass and all companies controlled by it, in accordance with the Reporting Management Procedure.

The **Reporting Team** presents the results of its investigation to the Supervisory Body and the Anti-Corruption Officer (if and to the extent relevant) before the final closure of the investigation, in order to gather any additional needs for further investigation. If the reports are unrelated to compliance with the "231" model or anti-corruption matters, the Reporting Team forwards them to the relevant department.

The Telepass Group ensures the confidentiality of the whistleblower's identity starting from the receipt of the report, in accordance with legal provisions.
In compliance with the law, Telepass prohibits and sanctions any form of retaliation or discrimination against anyone who has made a report, whether or not the report is subsequently proven to be valid. The prohibition of retaliation and the protection measures for the whistleblower also apply to:

- the facilitator (someone who assists the whistleblower in making the report);
- individuals related to the whistleblower by a stable personal or family relationship within the fourth degree;
- colleagues of the whistleblower who work in the same work environment and have a habitual and ongoing relationship with the whistleblower;

- entities owned by the whistleblower or for which they work, as well as entities operating within the same work environment as the whistleblower.

A "retaliatory act" is defined as any behaviour, act, or omission, even if attempted or threatened, carried out because of the report, the denunciation to the Judicial or Accounting Authority, or the public disclosure of the report, which causes or may cause unjust harm to the whistleblower or the person who made the report, either directly or indirectly. Retaliatory conduct is exemplified in Article 17, paragraph 4 of Legislative Decree no. 24/2023.

The absence of retaliatory intent in actions, acts, or omissions under Article 17 of Legislative Decree no. 24/2023 must be proven by the person who has carried out the action; in the absence of proof to the contrary, it is presumed that such actions are a consequence of the report.

All employees of the Telepass Group involved in the management of reports are required to maintain confidentiality regarding the existence and content of the report, as well as the identity of the individuals who reported and those reported. Furthermore, any violation of the whistleblower protection measures defined by the company or the submission, with intent or gross negligence, of unfounded reports, will result in disciplinary action.

It is emphasized that, both during the transmission and management of the reports, as well as during their archiving, appropriate technical and organizational measures are in place to ensure the security of personal data in compliance with privacy laws.

As for the content of the reports, they must relate to:

- violations (or suspected violations) of the Code of Ethics, the Model, the Anti-Corruption Policy, or the company's internal regulatory framework (policies, procedures, etc.);
- events that may cause financial or reputational harm to the Telepass Group;
- violations (or suspected violations) of national or European laws, as defined in Article 2, paragraph 1(a) of Legislative Decree no. 24/2023[7].

Finally, as required by law, reports should not concern personal grievances, claims, or requests related to the personal interests of the whistleblower.

[7] This specifically refers to: (i) administrative, accounting, civil, and criminal offenses that harm the interests, decorum, and integrity of the company; (ii) unlawful conduct relevant under Legislative Decree 231/01 or violations of the Organizational, Management, and Control Model; (iii) offenses falling within the scope of the European Directive regulating specific sectors such as public procurement, services, products, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, and data protection, as well as the security of networks and information systems; (iv) acts and omissions that harm the financial interests of the Union; (v) acts and omissions concerning the internal market of the European Union.

6. TRAINING

6.1 Employee Training

Employee training is a key requirement for the implementation of the Model. Telepass is committed to facilitating and promoting the knowledge of the Model among management and employees, with varying levels of depth depending on position and role, and their constructive contribution to the understanding of its principles and contents.

The principles and contents of Legislative Decree 231/2001 and the Model are communicated through mandatory training courses. The structure of these courses is approved by the Supervisory Body upon proposal from the relevant company functions.

The People and Organization function manages the training of the Company's personnel, disseminating knowledge of the Decree and the Model through a specific training plan and regularly providing the Supervisory Body with reports on such activities.

The traceability of participation in training sessions on the provisions of the Decree is ensured through the requirement for participants to sign an attendance sheet or, for e-learning activities, through the issuance of certificates of completion, or otherwise through other means of registering the completion of the course.

Any update training sessions, as well as specific information on the subject provided to new hires during the onboarding process, will be conducted in the event of significant changes to the Model, the Code of Ethics, or new relevant regulations affecting the Company's operations.

6.2 Information for collaborators and partners

Telepass promotes the knowledge and observance of the Code of Ethics and this General Section of the Model among commercial and financial partners, consultants, collaborators of any kind, customers, and suppliers of the Company. These documents are available on the Company's official website.

In order to formalize the commitment to comply with the principles of the Code of Ethics and this General Section of the Model by third parties with contractual relationships with the Company, a specific termination clause is included in the relevant contract. This clause grants the Company the right to terminate the contract by law and with immediate effect in the event of a breach of the Code of Ethics and/or this General Section of the Model by the contracting party.

Furthermore, the Company has adopted a series of protocols and procedures aimed at the better selection – also from an ethical and compliance perspective – of contractual counterparties.

In this way, Telepass pursues the objective of engaging with parties who share the Company's ethical principles and who pursue the same goal of legality.

7. DISCIPLINARY SYSTEM

Pursuant to Articles 6 and 7 of Legislative Decree 231/2001, for the effective implementation of the Model, a disciplinary system must be in place to sanction any failure to comply with the measures set out in the Model.

Telepass has therefore adopted a disciplinary system aimed at sanctioning violations of the principles and measures provided for in the Model and the corporate protocols, in compliance with applicable legal provisions and the regulations established by national collective bargaining, by the Recipients of the Model.

In accordance with Article 5 of the Decree, violations of the Model and the corporate protocols committed by individuals in Top Management positions as well as those who are subject to the direction or supervision of others or who operate in the name and/or on behalf of the Company are subject to sanctions. Additionally, this disciplinary system applies to any collaborators and partners of the Company.

The initiation of a disciplinary procedure and the possible application of sanctions is independent of whether a criminal proceeding is pending for the same act and does not depend on its outcome.

7.1 Relevant conduct

For the purposes of this Disciplinary System and in accordance with the provisions of collective bargaining agreements, relevant conduct, for the purpose of applying a possible sanction, includes actions or behaviours, including omissions, carried out in violation of the Model.

When determining the related sanction, both the objective and subjective aspects of the relevant conduct are considered. Specifically, the objective elements of the relevant conduct, ranked in increasing order of severity, are:

1. violations of the Model that did not expose the Company to risk or exposed it to only minor risk;
2. violations of the Model that resulted in considerable or significant exposure to risk;
3. violations of the Model that constituted a criminally relevant act.

A further violation of the Model is the failure to comply with the provisions relating to Whistleblowing under Legislative Decree No. 24/2023. Specifically, the following constitute violations of the Model:

- a false report made with intent or gross negligence, aimed at harming the whistleblower (so-called "bad faith" reporting);
- the implementation or threat of retaliatory measures against the whistleblower or other persons protected by the law;
- failure to protect the confidentiality of the whistleblower’s identity.

The severity of relevant conduct is further influenced by the subjective elements outlined below and, in general, by the circumstances in which the violation occurred. Specifically, in compliance with the principle of graduality and proportionality in determining the sanction to be imposed, the following factors are taken into account:

- the commission of multiple violations within the same conduct, in which case the aggravation will be applied based on the sanction for the most serious violation;

- the recidivism of the person(s) involved;
- the hierarchical and/or technical level of responsibility of the individual to whom the contested conduct is attributed;
- the possible sharing of responsibility with other individuals who contributed to the misconduct.

7.2 Sanctions for the Board of Directors[8] and members of the Board of Statutory Auditors

If a violation outlined in section 7.1[9] is committed by a Top Management, the following sanctions may be applied:

- formal written warning;
- a financial penalty, ranging from two to five times the monthly remuneration;
- removal from office.

The choice of the sanction to be imposed in the specific case will be based on the principles of proportionality and graduality identified in section 7.1.

7.3 Sanctions against Employees (managers[10], supervisors, administrative employees)

Failure to comply with and/or violations of the rules set out in the Model by employees of the Company constitutes a breach of the obligations arising from the employment relationship under Article 2104 of the Italian Civil Code and a disciplinary offense.

The adoption by an employee of the Company of conduct that qualifies, as indicated in the previous paragraph, as a disciplinary offense also constitutes a violation of the employees' obligation to perform their duties with the utmost diligence, following the directives of the Company, as provided by the applicable Collective Labor Agreement (CCL), as well as by the provisions of the Disciplinary Code.

Sanctions are applied based on the significance of each specific case considered and are proportional to their severity, in accordance with what is set out in the previous paragraph 7.1.

If a violation of the Model attributable to the employee is established[11], and considering the provisions of Article 7 of Law No. 300/1970 and the applicable CCL, the following disciplinary measures may be applied:

---

[8] Limited to the Directors who do not have an employment relationship.

[9] By way of example and without limitation to what is indicated in the previous paragraph 7.1, the following types of conduct may constitute the grounds for the application of the sanctions outlined below:

- failure to comply with the principles and protocols set out in the Model;
- violation and/or circumvention of the control system, carried out through the removal, destruction, or alteration of documentation required by the company protocols, or by obstructing authorized persons and the Supervisory Body (SB) from carrying out control or accessing the requested information and documentation;
- violation of the provisions regarding signature powers and, in general, the delegation system, except in cases of necessity and urgency, in which case timely information must be provided to the Board of Directors;
- violation of the duty to inform the SB and/or any superior officer regarding behaviours aimed at the commission of a crime or an administrative offense included among those provided for by the Decree.

[10] The sanctioning criteria and the disciplinary procedure take into account the type of employment relationship between these individuals and the Company.

[11] By way of purely illustrative and non-exhaustive example of what is indicated in the previous paragraph 7.1, and subject to the provisions of the applicable CCL for the application of potential disciplinary measures, the following are some relevant behaviours:

1) conservative disciplinary measures:
    a. verbal reprimand;
    b. written reprimand;
    c. a fine not exceeding four hours of the global daily salary as per point 1 of Article 22
    d. suspension from service and pay for up to 10 days (for part-time employees, up to 50 hours);
2) disciplinary measures resulting in termination:
    a. dismissal with notice;
    b. dismissal without notice.

Without prejudice to the provisions of the applicable CCL and the Disciplinary Code, the choice of the sanction to be applied in the specific case will be made based on the principles of proportionality and graduality as identified in paragraph 7.1.

If the nature of the offense affects the trust-based relationship, it will be possible to proceed with the precautionary suspension of the employee pending appropriate investigations.

As for managerial staff, given the highly fiduciary nature of the relationship and considering that managers carry out their functions in order to promote, coordinate, and manage the achievement of the company's objectives, violations of the Model will be assessed in relation to collective bargaining agreements, in line with the specificities of the managerial relationship.

7.4 **Sanctions Applicable to Third-Party Recipients**

The present Disciplinary System serves to sanction violations of the Code of Ethics and the Model committed by Third-Party Addressees.

This category may include:

- those who have a contractual relationship with Telepass (e.g., consultants, professionals, etc.);
- those responsible for auditing and accounting control;
- collaborators in any capacity;
- attorneys and individuals acting in the name and/or on behalf of the Company;
- suppliers and partners.

- violation of internal procedures or the adoption, in the performance of high-risk activities, of conduct that is inconsistent with the provisions of the Model itself, such conduct being considered as non-compliance with orders given by the Company, both in written and verbal form (e.g., an employee who fails to follow prescribed procedures, omits to inform the Supervisory Body of the required information, fails to carry out checks, etc.);
- adoption, in the performance of high-risk activities, of conduct that is inconsistent with the provisions of the Model or a violation of its principles, such conduct being considered as non-compliance with orders given by the Company (e.g., an employee who refuses to undergo medical checks as per Article 5 of Law No. 300 of May 20, 1970; falsifies and/or alters internal or external documents; deliberately fails to apply the directives issued by the Company in order to gain an advantage for themselves or for the Company; is a repeat offender of any of the misconducts that led to the application of conservative disciplinary measures).

Any violation committed by the aforementioned individuals may result in the application of penalties or the termination of the contractual relationship, depending on the violation in question and the level of risk to which the Company is exposed.

7.5 Investigative procedure

The procedure for the imposition of sanctions consists of:

- the investigative phase;
- the phase of notifying the alleged violation to the person concerned;
- the phase of determining and subsequently imposing the sanction.

The investigative phase begins based on the verification and inspection activities carried out by the Supervisory Body, which, following its investigative activities or the analysis of the reports received, promptly informs and then submits a written report to the person with disciplinary authority, as identified below, regarding any identified violation and the person(s) responsible for it.

Investigative procedure concerning members of the Board of Directors

If the Supervisory Body identifies a violation of the Model by one or more individuals holding the office of Director, who are not bound by an employment relationship with the Company[12], the Supervisory Body shall forward a report to the Board of Directors and the Board of Statutory Auditors containing:

- a description of the contested conduct;
- an indication of the provisions of the Model that have been violated;
- the individual responsible for the violation;
- any documents proving the violation and/or other corroborating elements.

Following the receipt of the Supervisory Body's report, the Board of Directors will convene the Director to whom the violation is attributed. The convocation must:

- be made in writing;
- include the description of the contested conduct and the provisions of the Model that have been violated;
- inform the individual concerned of the date of the meeting, with notice of their right to submit any observations and/or defenses, either written or verbal.

The convocation must be made according to the established procedures for convening the Board of Directors.

During the Board of Directors' meeting, at which the Supervisory Body is also invited to participate, the hearing of the concerned individual will take place, along with the consideration of any observations submitted by them and the carrying out of any further investigations deemed necessary.

[12] In the event that the violation of the Model is attributable to a Director who has an employment relationship with the Company, the authority to impose disciplinary measures lies with the Board of Directors, and the investigation and possible contestation procedure shall be subject to the safeguards provided for under Article 7 of Law No. 300/1970 and the applicable CCNL.

The Board of Directors, with the abstention of the concerned director, shall assess the validity of the acquired evidence and, in accordance with Articles 2392 and following of the Italian Civil Code, convene the Shareholders' Meeting to make the necessary determinations.

The decision of the Board of Directors, in the case of unfounded allegations, or that of the convened Shareholders' Meeting, shall be communicated in writing by the Board of Directors to the concerned individual and to the Supervisory Body.

If the Supervisory Body identifies a violation of the Model by the entire Board of Directors or by the majority of the Directors, the Supervisory Body shall inform the Board of Statutory Auditors so that it may promptly convene the Shareholders' Meeting for appropriate measures.

Investigative procedure for the Statutory Auditors

In the event of a violation of this Model by a Statutory Auditor, the Supervisory Body shall inform the entire Board of Statutory Auditors and the Board of Directors of the Company, through their respective Presidents, by means of a report containing:

- a description of the contested conduct;
- an indication of the provisions of the Model that have been violated;
- the identification of the person responsible for the violation;
- any documents supporting the violation and/or other relevant evidence.

Following the receipt of the Supervisory Body's report, the Board of Statutory Auditors, in a joint meeting with the Board of Directors, shall convene the Statutory Auditor concerned to address the alleged violation.

The notice of the meeting must:

- be issued in writing;
- indicate the contested conduct and the provisions of the Model that have been violated;
- inform the individual of the date of the meeting, with the right to make any comments and/or submissions, both written and oral.

The notice must be given in accordance with the established procedures for convening the Board of Directors.

The Board of Directors of the Company, after assessing the significance of the report, shall activate the Shareholders' Meeting for the appropriate decisions.

If the Supervisory Body identifies a violation of the Model by multiple Statutory Auditors or the entire Board of Statutory Auditors, it shall inform the Board of Directors so that it may promptly convene the Shareholders' Meeting to take the necessary actions.

Investigative procedure for Employees (managers, supervisors, administrative employees)

In the event of a violation of the Model by an employee, the procedure for verifying the violation is carried out in compliance with the applicable legal provisions as well as the applicable collective labor agreement.

In particular, the Supervisory Body submits a report to the CEO containing:

- a description of the contested conduct;

- an indication of the provisions of the Model that have been violated;
- the identification of the person responsible for the violation;
- any documents supporting the violation and/or other relevant evidence.

Following the receipt of the Supervisory Body's report, the CEO summons the person concerned by sending a formal written notice of the violation containing:

- a description of the contested conduct and the provisions of the Model that have been violated;
- the time frame within which the person concerned may submit any comments and/or defenses, both written and oral.

If the person concerned wishes to respond orally to the notice, the Supervisory Body is invited to attend the meeting. During this meeting, any points raised by the individual will be recorded.

At the conclusion of the activities outlined above, the CEO will decide whether to impose a sanction and will determine the specific sanction to be applied.

The decision to impose a sanction, if applicable, is communicated in writing to the person concerned, in accordance with any time frames set by the applicable collective labor agreement.

The relevant departments are responsible for ensuring the effective imposition of the sanction, in compliance with legal and regulatory requirements, as well as the provisions of the applicable collective labor agreement and company regulations, where applicable.

The Supervisory Body is notified, for information purposes, of the decision to impose a sanction.

Investigative Procedure for Third Parties

In order to enable the adoption of the measures outlined in the above-mentioned contractual clauses aimed at ensuring compliance with the principles of the Ethical Code and the present General Section of the Model by third parties with contractual relationships with the Company, the Supervisory Body submits a report to the responsible head of the business unit/department managing the contractual relationship. The report shall contain:

- the identification details of the party responsible for the violation;
- a description of the contested conduct;
- the identification of the provisions of the Ethical Code and the present General Section of the Model that have been violated;
- any documents supporting the violation and/or other relevant evidence.

This report, if the contract was approved by the Board of Directors, must also be forwarded to the attention of the Board of Directors and the Board of Statutory Auditors.

The head of the business unit/department managing the contractual relationship, in agreement with the Legal Affairs Department, if requested, shall send a written communication to the party concerned. This communication shall include a description of the identified conduct, the provisions that have been violated, and an indication of the specific contractual clauses included in the engagement letters, contracts, or partnership agreements that are intended to be applied.