ORGANISATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE 231/01

Revision No. 0 Adoption of the Organisation and Management Model, approved by resolution of the Board of Directors on ....

TABLE OF CONTENTS

GLOSSARY

- ***Managing Director***: the Company CEO
- ***Risk Areas***: areas of activity considered to be vulnerable to the risk of commission of offences pursuant to Legislative Decree 231/2001 ("at risk" activities).
- ***Sensitive Processes:*** activities of the company that are vulnerable to the risk of commission of Offences.
- ***c.c.*** Civil Code
- ***p.c.*** Penal Code
- ***BoD***: the Board of Directors of the Company.
- ***CCNL***: the National Collective Labor Agreement by which the company regulates relations with its employees.
- ***Code of Ethics***: a document that identifies the set of values and rules of conduct to which the company intends to make continuous reference in the performance of its activities.
- ***Collaborators***: persons who provide their services to the Company on an ongoing basis and in coordination with the Company, independently of any relationship of employment or subordination.
- ***Consultants***: persons who act in the name and/or on behalf of the company based on a mandate or other professional collaborative arrangement.
- ***Recipients***: (i) the governing and corporate bodies and officers and all those who hold representation, management (including de facto) and administrative functions in the company, (ii) employees of the company (seconded or otherwise), including managers, (iii) non-company collaborators (such as professionals and consultants, including companies, trainees, interns etc.) of the Company.
- ***Employees***: all persons bound by a formal employment relationship with the company.
- ***Legislative Decree 231/2001 (the 'Decree', below):*** Legislative Decree no. 231 of 8 June 2001, entitled *"Regime of administrative liability attributable to legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law no. 300 of 29 September 2000",* as amended.
- ***ESG***: Environmental, Social, Governance sustainability criteria.

- ***Entities***: legal persons to which the regime of Legislative Decree 231/2001 applies.
- ***Guidelines:*** Guidelines for the drafting of organisation, management and control models pursuant to Legislative Decree 231/2001, most recently updated by Confindustria in June 2021.
- ***Organisation Model, or Model:*** the Organisation, Management and Control Model provided for by Legislative Decree 231/2001.
- ***Governing Bodies:*** the Board of Directors, the Board of Statutory Auditors and the Shareholders' Meeting.
- ***Supervisory Body*** or ***SB***: the internal body in charge of supervising the operation of and compliance with the Model and its updating, vested with independent powers of initiative and control.
- ***PA***: the Public Administration i.e. public bodies and/or persons treated as such (e.g. holders of a public service) regulated by the Italian State, by the EU, by foreign States and/or under international law and, in relation to offences against the public administration, public officials and public service officers working for them.
- ***Partners***: the Company's contractual counterparties, such as service companies, agents, partners, whether natural or legal persons, with whom the Company reaches any form of collaboration arrangement regulated by contract and who are to collaborate in activities that constitute Sensitive Processes.
- ***Procedures***: documents of various kinds (e.g. instructions, rules) aimed at defining how a specific activity or process is to be carried out.
- ***Protocols***: a set of company prevention rules and standards such as, for example, procedures, operating rules, manuals, forms and communications to personnel.
- ***Units***: a measure referenced in Legislative Decree 231/2001 for calculating monetary penalties.
- ***Offences or predicate offences***: the offence categories that are a prerequisite for an entity to be held administratively liable under Legislative Decree 231/2001.
- ***Senior Managers:*** persons who hold representation, administration or management positions within GIMA S.p.A. or one of its financially and functionally independent organisational units, and those who exercise (also de facto) management and control powers in the entity.

- ***Subordinate Persons:*** persons, within GIMA S.p.A., who are subject to the management or supervision of a Senior Manager.
- ***Company*** or ***GIMA:*** the company *GIMA S.p.A.* with registered office in Gessate (MI), via Marconi n. 1.
- ***Third Parties:*** persons involved in relevant dealings with GIMA S.p.A. (e.g. stakeholders, suppliers, auditing companies, consultants, collaborators, etc.).
- ***Whistleblowing***: a mechanism by which employees and/or non-company collaborators, Partners, Consultants or suppliers are, by reason of the functions performed, duty-bound to report any unlawful conduct through special company channels, if evidence should come to light - based on precise and concordant facts - of infringements and/or possible infringements of the Model, of the Code of Ethics, of internal company and group rules, and of any other regulation or standard (also external) applicable and relevant to the Company.

GENERAL PART

1. THE REGIME OF ADMINISTRATIVE LIABILITY OF LEGAL PERSONS, COMPANIES AND ASSOCIATIONS

1.1 Legal framework

Legislative Decree 231/01 (hereinafter 'the 231 Decree' or 'the Decree') - "*Regulating the administrative liability of legal persons, companies and associations, including entities without legal personality*" - first introduced into Italian law the concept of the criminal liability of entities for administrative offences arising from the commission of a criminal offence.

This particular form of liability is administrative in name, but is essentially punitive-criminal in nature, and applies to companies, associations and entities in general where specific criminal and administrative offenses are committed in their interest or to their advantage by natural persons holding senior management or subordinate positions within these entities.

The 231 Decree represents a major regulatory intervention that superimposes the entity's "administrative" liability over the criminal liability of the natural person who actually committed the offence, provided that the legal requirements referred to therein are met.

The provisions of Article 1, paragraph II, of the Decree apply to:

- entities with legal personality;
- companies and associations, including those without legal personality.

Pursuant to the subsequent paragraph III, the following entities are, however, excluded from the provisions in question:

- the State;
- local public bodies;
- not-for-profit public bodies;
- entities performing functions of constitutional importance.

Liability is attributable to the entity where the offences, indicated by the Decree, have been committed by persons linked in various ways to the entity.

Article 5 of the Decree indicates the following as perpetrators of the criminal offence:

- persons who hold representation, administration or management positions within the entity or one of its financially and functionally independent organisational units, and those who exercise (de facto) management and control powers in the entity (Senior Managers);
- persons who are subject to the management or supervision of senior managers (Subordinate Persons).

Recognition of the entity's liability also presupposes that the unlawful conduct was carried out by the above-mentioned persons '*in the interest or to the advantage of the Company*' within the meaning of Article 5(I) of the Decree (applying the objective imputation criterion).

The two requirements of interest and advantage are independent and do not overlap.

In particular, in the interpretation of the case law of the Italian Supreme Court of Cassation, the interest must consist of an resultant undue enrichment of the entity that is planned, even if not achieved; the criterion used by the courts is subjective and, accordingly, the court must determine the existence of this requirement *ex ante*, by reference to the moment when the criminal action took place.

The second requirement has been identified as a benefit or advantage objectively resulting from the commission of the offence, even if not actually envisaged or planned; this is an essentially objective component which, as such, must be verified *ex post* by reference to the actual effects or results of the offence.

Under Article 5, para. II. of the Decree, the entity will not be liable if the senior managers or subordinate persons have acted *'in their own exclusive interest or in the interest of third parties'.*

1.2 Predicate offences in general

Entities are not called to account for every offence committed by senior managers or subordinate persons, but only for those strictly provided for by the Decree and, specifically, for the offences listed below:

1. offences committed in dealings with the Public Administration (Arts. 24 and 25 of the Decree);
2. computer offences and unlawful processing of data (Art. 24-bis of the Decree);
3. organised crimes (Art. 24-ter of the Decree);
4. offences of falsification of currency, public credit notes, official stamps and identification instruments or marks (Art. 25-bis of the Decree);
5. offences against industry and commerce (Art. 25-bis.1 of the Decree);
6. corporate offenses (Art. 25-ter of the Decree);
7. crimes aimed at terrorism and subversion of the democratic order (Art. 25-quater of the Decree);
8. crimes of infibulation (female genital mutilation) (Art. 25-quater.1 of the Decree);
9. offences against personal dignity (Art. 25-quinquies of the Decree);
10. offences of market abuse (Art. 25-sexies of the Decree);
11. offences of manslaughter and serious or grievous injury committed in violation of workplace health and safety rules (Article 25-septies of the Decree);
12. crimes of receiving stolen goods, money-laundering, use of money, goods or economic benefits of illicit origin, and self-laundering (Art. 25-octies of the Decree);
13. offences involving non-cash payment instruments (Art. 25-octies.1 of the Decree);
14. copyright infringement offences (Art. 25-novies of the Decree);
15. crimes of inducement not to make statements, or to make false statements to the judicial authorities (Art. 25-decies of the Decree);
16. environmental offences (Art. 25-undecies of the Decree);
17. offences of recruitment of undocumented third country nationals (Article 25-duodecies of the Decree);
18. crimes of racism and xenophobia (Art. 25-terdecies of the Decree);
19. crimes of fraud in sports competitions, illegal gaming, gambling and betting and gambling using prohibited devices (Art. 25-quaterdecies of the Decree);
20. tax offences (Art. 25-quinquiesdecies of the Decree);
21. smuggling offences (Art. 25-sexiesdecies of the Decree);
22. crimes against cultural heritage assets (Art. 25-septiesdecies of the Decree);
23. crimes of laundering of cultural heritage assets and depredation and looting of cultural and landscape heritage assets (Art. 25-duodecies of the Decree);

24. cross-border offences, introduced by Law no. 146 of 16 March 2006, '*Law ratifying and implementing the United Nations International Convention and Protocols against Transnational Organised Crime'.*

1.3 Offences committed abroad

Article 4 of the Decree provides that organisations are also liable for offences committed abroad, on the twofold condition that they have their principal place of business in Italy and that the cases and further conditions provided for in Articles 7, 8, 9 and 10 of the Italian Penal Code are met, so that citizens and foreigners are subject to punishment under Italian law for offences committed on foreign soil.

The article also provides that entities will be prosecuted on condition that the State of the place where the offence was committed does not proceed against them. Lastly, the article provides that, in cases where the perpetrator is punished at the request of the Minister of Justice, proceedings will be brought against the entity only if the request is also made against the latter.

The rules laid down by Article 4 of the Decree and by the relevant provisions of the Penal Code only concern offences committed abroad in their entirety, by persons having the characteristics set out in Article 5(I) of the Decree and belonging to entities having their principal place of business in Italy. Moreover, for most of the offences provided for in the Decree, the liability to punishment of such persons and of the entity would depend on the Minister of Justice request.

In summary, the prerequisites necessary for the applicability of Article 4 above, and therefore for the entity's liability to punishment for offences under the Decree, are:

1. the offence must be committed abroad by a person functionally linked to the entity;
2. the entity must have its principal place of business in Italy;
3. the entity may be liable in the cases and under the conditions set out in Articles 7, 8, 9 and 10 of the Penal Code;
4. in the cases and conditions indicated in para. 3), the entity is liable provided that proceedings are not brought in the State where the offence was committed;
5. in cases where the perpetrator is punished at the request of the Minister of Justice, proceedings will be brought against the entity only if the request is also made against the latter;

6. the perpetrator must be in the territory of the State at the time the criminal proceedings are prosecuted, and must not have been extradited.

1.4 Sanctions

The Decree provides for the following system of penalties:

- monetary penalties;
- disqualification penalties;
- confiscation;
- publication of the judgment.

Their application against the entity varies depending on the individual predicate offence committed.

The court calculates the monetary penalty by taking into account the seriousness of the offence, the degree of the entity's liability and also any actions it took to eliminate or mitigate the consequences of the offence and prevent the commission of further offences.

Disqualification penalties, on the other hand, may include:

- disqualification from the business activity;
- suspension or revocation of authorisations, licenses or concessions that facilitate the commission of the offence;
- prohibition on contracting with the public administration except to obtain the performance of a public service;
- exclusion from financial facilities, loans, grants or subsidies and revocation, as appropriate, of those already granted;
- prohibition on advertising goods or services.

Disqualification penalties, which are applicable in interlocutory proceedings, may have a duration of no less than three months and no more than two years, except in the case of offences against the Public Administration, pursuant to Article 25, paragraphs II and III of the Decree, for which the recent Law no 3 of 9 January 2019, - entitled '*Measures to combat offences against the public administration, and related to the statute of limitations for the offence and the transparency of political parties and movements'* - has increased the monetary penalty by

establishing that, if the offence is committed by a Senior Manager the duration cannot be less than four years or more than seven years whereas, if the offence is committed by a subordinate person, it cannot be less than two years or not more than four years.

At the same time, in order to prevent disqualification penalties from being too lengthy where they are granted at the interlocutory stage (Article 45 of the Decree), the new law amended the provisions of Article 51 by indicating the maximum term of disqualification penalties that can be handed down in interim proceedings: namely a fixed duration of one year for an interim measure ordered by the court, and of one year and four months for the duration of the interim measure after a criminal conviction at first instance.

Furthermore, pursuant to Article 50 of the Decree, interlocutory measures ordered against entities must be revoked - including by the court of its own motion - not only when the conditions of applicability pursuant to Article 45 are found wanting (also due to the presence of supervening events), but also when the specific circumstances are present which are envisaged by Article 17 of the Decree, which regulates cases when the adverse consequences of the predicate offence are mitigated or redressed, for specific purposes of prevention.

Accordingly, Law 3/2019 acknowledged the entity's collaboration in the proceedings by establishing, in Article 25, paragraph V-bis of the Decree, a mitigated disqualification penalty (not less than three months and not more than two years) in cases where the entity, prior to the court sentence of first instance, has taken effective steps to prevent the criminal activity from being taken further, has taken steps to obtain evidence of the offenses and to identify the perpetrators or to seize the sums or profits arising from the offence, and has eliminated the organisational failures that facilitated the criminal offense being committed in the first place, by adopting and implementing a model of organisation, management and control suitable for preventing criminal offenses of the kind that occurred.

1.5 Attempted offences

In the event of attempted commission of the offences specified in Chapter I of the Decree (articles 24 to 25-octies), the monetary penalties and the disqualification penalties are reduced by between one third and one half, while penalties are excluded if the company of its own initiative prevents the action from being carried out or the event from taking place (Article 26). In such instances, the non-application of sanctions is justified by the cessation of any

relationship of organic identity between the entity and the individuals purporting to act in its name and on its behalf.

1.6 Prerequisites for the exclusion of the Entity's liability

Article 6 of the Decree provides that entities can be exempt from liability for offences committed by persons in senior management positions if the entity can prove that:

- the Board of Directors adopted and effectively implemented - prior to the offence - organisation, management and control models suitable for preventing the commission of offences;
- an internal organ with independent powers of initiative and control (i.e. the supervisory body) has been charged with overseeing the operation of and compliance with the models, and updating them;
- the offence was committed by fraudulently circumventing the existing model;
- the supervisory body was not responsible for any non-existent or inadequate oversight.

Where an offence is committed by a person in a subordinate position, Article 7 of the Decree makes the exclusion of the entity's liability conditional on the effective implementation of an organisational, management, and control model that is suitable - given the type of organisation and the activity carried out - for ensuring compliance with the law, and for preventing situations from arising that are “at-risk” for the Company i.e. vulnerable to the commission of offences under the Decree.

The Decree also provides that organisation, management and control models must:

- identify the activities within the scope of which offences under the Decree may be committed;
- establish specific prevention standards (called ‘protocols’ below) that can guide the process in and through which company decisions are formed and implemented;
- identify methods for managing financial resources suitable to prevent the commission of offences under the Decree;
- establish obligations to provide information on major corporate events to the Supervisory Body, and in particular on the activities deemed to be at risk;

- introduce disciplinary systems suitable for sanctioning non-compliance with the measures indicated in the model.

Moreover, pursuant to Article 6, paragraph II-bis of the Decree, organisation, management and control models must provide for internal reporting channels, a prohibition against retaliation and the above-mentioned disciplinary system, pursuant to Legislative Decree 24/2023 on whistleblowing.

1.7 Confindustria Guidelines

Article 6, paragraph III of the Decree states that '*Organisation and management models may be adopted, ensuring the requirements pursuant to paragraph 2, based on codes of conduct that have been drawn up by associations representing the entities and communicated to the Ministry of Justice which, in agreement with the competent Ministries, may - within thirty days - make observations on the suitability of the models to prevent offences'.*

This Model was developed by taking into consideration the demands of the specific context in which the Company operates and, therefore, the requirements dictated by operational processes linked to the description in the Confindustria Guidelines. The Guidelines are for reference purposes only and are therefore not prescriptive or mandatory in nature, but they are among the documents envisaged by Article 6, para. III, of Legislative Decree 231/2001, which expressly provides that organisational, management and control models may be adopted based on codes of conduct drawn up by associations that represent Entities.

As reiterated by the Guidelines, models should be devised and implemented in a way that resonates with the purposes and requirements of the Decree, namely the concrete (and not merely theoretical) prevention of offense risk that relates to the company's concrete situation and business reality, so that the model can become effectively and constructively integrated in its day-to-day processes and operations.

The Guidelines recommend creating a model only after the entity's organisational structure has been thoroughly and comprehensively assessed, so as to be able to identify the areas and activities that are vulnerable to the commission of offences envisaged by the Decree.

The Guidelines recommended that the following key elements need to be examined closely for prevention purposes:

- the list of criminal and other offences considered by Legislative Decree 231/01;
- the description of the entity's organisation as a whole;
- the areas and activities within the entity's remit that are vulnerable to the commission of offences under the Decree and could also trigger liability for the entity;
- the conferment of powers of attorney, delegated powers and corporate powers and the extension thereof, obviously in relation to the offences considered by the Decree;
- the avoidance of excessive concentrations of power in individuals or individual offices;
- the guarantee of a clear and organic allocation of tasks;
- the guarantee that organisational resources are effectively activated;
- the clear and exhaustive definition of the procedures to be followed for taking decisions that fall within the entity's responsibility, and that may expose it to liability under the Legislative Decree 231/01;
- the processes and forms of protection provided by the Model's provisions, so as to avoid their circumvention;
- the guarantee of procedures for control and transparency in the formation and management of funds;
- the requirement that all persons interacting within the entity should observe mandatory processes of timely information provision to the Supervisory Body;
- the involvement of all personnel and external collaborators in the task of compliance with the Model's provisions, for example by looking at a system for reporting infringements thereof directly to the SB;
- the planning and holding of special training courses for personnel and others who are subject to the management or supervision of the entity, and their familiarisation with the risk of commission of the criminal and other offences contemplated by the Decree;
- the procedures for the imposition of suitable sanctions for non-compliance with the model's provisions;
- effective processes to spread awareness among employees and collaborators of the principles that guided the Model's implementation;
- the drafting and application of a clause, in contracts that regulate dealings between the Entity and individuals working in its organisation, by which the signatories declare their familiarity with the model or, as a minimum, with the guiding principles that inspired it;
- the processes and templates for the continuous auditing and updating of the model.

2. PRESENTATION OF THE COMPANY

GIMA is an Italian leader in the production and marketing of medical items, with over 97 years of experience and a network of distributors present in over 145 countries worldwide.
Having been a distributor of important English, American and German brands on the Italian territory for many years, GIMA has in recent years created several product lines under its own brand.
Its offer covers various medical specialities, in particular gynaecology, dermatology, vascular surgery, general surgery, ENT, veterinary medicine and paediatrics.

The company, manages the compliance with all mandatory regulations (those referable to Legislative Decree 81/2008, or to EU Regulation 679/2016 and Legislative Decree 24/2023)

The Company has adopted various management systems and, consequently, must comply with the many mandatory provisions of regulations dealing with work safety, environmental prevention, respect for privacy, organisational management models, quality management and data and information security.
For this reason, the management has decided to integrate the various activities, within the processes controlled by this Integrated Management System, considering the following requirements:

- Company context;
- Management, policy and responsibilities;
- Processes for planning and considering risks and opportunities;
- Processes relating to customers, products and services;
- Processes for improvement.

2.1 The governance system : roles, duties and responsibilities

The company was founded in 1926 under the name *G.I.M.A.* (*Gruppo Industriale Milanese Aghi*) dedicated to the production of needles and glass syringes.
In 1955, the company was taken over by *Attilio Manzoni* who established *GIMA S.p.A.* on 9 September 1955.

The subscribed and paid-up share capital currently stands at EUR 364,000.00.

The company is organisationally structured according to a logic of functional roles and responsibilities and the company organisation chart displays the corresponding hierarchical levels.

The organisation in terms of roles, duties and responsibilities is described in detail in the updated version of the organisation chart, attached to this Model, according to a hierarchical/functional arrangement. Job duties and operational roles are based on documents that describe the associated job duties and tasks.

The company search record (Chamber of Commerce) may be consulted to check who holds company representation and administrative functions or other corporate offices or positions (such as special representatives and technical managers); it indicates the individual powers for the following corporate figures:

- Chairperson of the Board of Directors;
- Managing Director;
- Directors;
- Auditors;
- External Audit Firm;
- Special representatives.

However, the roles and responsibilities of these individual figures are based not only on the provisions of internal documentation and procedures, but on all mandatory rules applicable.

3. THE ORGANIZATION, MANAGEMENT AND CONTROL MODEL of GIMA S.P.A.

3.1 Purposes of the Organisation, Management and Control Model of GIMA S.P.A.

In order to improve the overall organisation and management of the Company and to prevent the risk of commission of offences deemed attributable, in principle, to its corporate activities, GIMA has adopted an Organisation, Management and Control Model, divided into the following parts:

i) an *institutional structure* and an *organisational structure*, consistent with the nature and size of the organisation and with the type of activity carried out (see the corporate purpose), that:

(1) ensures the performance of the company's activities in compliance with law; (2) identifies and eliminates vulnerabilities (i.e. risk situations) in good time; (3) clearly identifies top or Senior Management functions and circumscribes their remit; (4) transparently represents the process in and through which company decisions are formed and implemented;

ii) the *Code of Ethics*, aimed at establishing the ethical principles and rules of conduct that inspire or ought to inspire the conduct of all persons operating in GIMA;

iii) the *operating instructions and procedures,* aimed at regulating business or corporate processes that have been identified as *sensitive*, i.e. entailing a potential risk of commission of certain predicate offences referenced in the Decree;

iv) the *corporate governance* rules, adopted in implementation of applicable company regulations, and any other documentation, relating to the control systems in place at the Company;

v) the *information flow system*, aimed at tracking the actions of individual corporate functions, so as to ensure the monitoring of processes that are potentially sensitive or at risk;

vi) the *information and training system*, which concerns the organisation, management and control Model adopted;

vii) the *disciplinary system,* aimed at sanctioning the violation or non-application of the Model by Recipients;

viii) the establishment of a *Supervisory Body*, vested with independent decision-making and spending authority and tasked with overseeing the operation of and compliance with the *Organisation Model* adopted, and also ensuring that it is updated.

When drafting the Organisation, Management and Control Model, account was taken of the procedures and control systems already in place in the Company, which also effectively operated as measures to prevent the commission of offences under the Decree.

The rules, operating instructions and procedures listed above are detailed in this Model but, instead, are integrated into the Company's broader organisation and internal control system, to

which the Organisation Model refers and which all Recipients are required to respect, based on their respective specific relationships with GIMA.

3.2 Structure of the Organisation, Management and Control Model

This document consists of a "General Part", individual "Special Parts", and annexes.

The ***General Part*** defines the structure of the Organisation Model: i) by regulating its purposes and functions; ii) by establishing a Supervisory Body and describing its functions and powers in the special Rules annexed; iii) by creating a system of information flows; iv) by creating an information and training system; v) by establishing a disciplinary system suitable for sanctioning non-compliance with the Model.

The ***Special Parts*** are identified by reference to the types of offences provided for in the Decree, whose commission is considered, in theory, to be more likely in view of GIMA S.p.A.'s typical corporate activities.

The ***Annexes*** include the: i) Code of Ethics; ii) company organisation chart; iii) whistleblowing procedure.

Of course the risk remains that, where new types of offence under the Decree are introduced in the context of regulatory changes, the Company may fail to promptly update its risk mapping activity and revise its existing organisational and control measures, in order to ascertain whether the company harbours a potential risk of that the recently introduced types of offences may in fact be committed.

In light of the foregoing, the Board of Directors, also taking into account the suggestions and indications provided by the appointed Supervisory Body, will, if the need arises, draw up new sections of the Special Part, formalising through specific resolutions the additions and/or changes made.

3.3 Recipients of the Organisation, Management and Control Model

The Organisation, Management and Control Model applies to:

- persons in senior management positions, reporting to GIMA S.p.A. (persons holding representative, administrative or management functions of the Company) and to persons who implement such powers (including *de facto*);
- persons who are subject to the direction or supervision of superiors ('subordinate' persons), reporting to GIMA S.p.A., namely persons who implement senior management decisions in the interest of the Company (i.e. GIMA S.p.A. employees);
- authorised representatives who operate in the name and on behalf of GIMA S.p.A.;
- members of the Board of Statutory Auditors;
- persons/companies/entities that provide services for the Company, under formally signed contracts, within the limits of the agreed provisions.

3.4 Amendments and additions to the Organisation, Management and Control Model

Article 6(I) of the Decree provides that the Organisation, Management and Control Model must be adopted and effectively implemented by the '*Management Body*'.

This article dictates, therefore, that any substantive amendment and supplement to the Model must be referred to the exclusive competence of GIMA S.p.A.'s Board of Directors.

It is acknowledged, however, that the Chairperson and/or Managing Director is empowered to make formal amendments or additions to the text.

In such a case, the Chairperson and/or Managing Director will report to the Board of Directors on any changes introduced.

The Supervisory Body is empowered to propose to the Chairperson and the Managing Director any additions and/or amendments to this Model.

Depending on the type of amendment proposed, it will be communicated directly to the Chairperson and/or Managing Director or submitted by the latter to the Board of Directors for approval.

3.5 Function and effectiveness of the Model

The adoption and effective implementation of the Model not only enables GIMA S.p.A. to avail of the exemption under the Decree in the event of a finding of administrative liability pursuant

to that Legislative Decree 231/01 but, within the limits thereof, it also fortifies the Company's internal control system by limiting the risk of offences under the Decree being committed.

In fact, the purpose of the Model is to put in place a structured, cohesive and organic system of preventive control procedures and processes, the aim of which is to prevent the commission of offences under the Decree, by identifying Sensitive Processes within the company and ensuring they are brought into line under special prevention procedures.

Accordingly, activities which due to their intrinsic nature are considered to be more vulnerable to the commission of offences under the Legislative Decree 231/01 are listed in detail in the Special Part of the Model.

The Supervisory Body also has authority to identify additional Sensitive Processes for inclusion in this list, where necessitated by legislative changes or by the evolution of company activities.

The principles enshrined in this Model must, on the one hand, aim to ensure that potential offenders are made aware that an offence is involved (in violation of company prohibitions and contrary to the Company's interest, even where it could stand to benefit from such offence), but the principles should also - due to continuous checks and monitoring - enable the Company to react promptly to pre-empt or prevent the commission of such offence.

The purposes of the Model, therefore, include the awareness-raising of employees and of the governing and corporate bodies operating on behalf or in the interest of the company within the context of Sensitive Processes, that if their conduct should fail to comply with the Model's requirements and with other company procedures in place (or, *a fortiori,* with law), they could be guilty of committing offenses that have criminal consequences not only for themselves but also for the Company.

The Company also intends to actively combat illegal conduct through the Supervisory Body's ongoing oversight of the actions of Recipients in the context of Sensitive Processes, and the possible imposition of disciplinary sanctions or contractual penalties.

3.6 Adoption of the Model for subsidiaries and associated entities

If GIMA S.p.A. should establish any Italian companies or entities (directly or indirectly controlled) or participate in any companies or entities, it will spearhead a dedicated organisational arrangement to ensure compliance with its own Organisation, Management and

Control Model (pursuant to the Legislative Decree 231/01) and with the requirements of the Decree itself.
Any new Italian subsidiaries will, through the competent departments, be required to inform GIMA S.p.A. that they have adopted an organisation model and appointed a supervisory body in conformity with the Decree and with best practices.
Should it be necessary to set up various associative entities in the course of its operations, these entities, as well as any Partners involved in them, shall be required to make a special formal declaration attesting to their knowledge of all of the provisions of GIMA S.p.A.'s Organisation Model (clause 231/01).
With regard to participatory relationships with foreign companies, GIMA S.p.A. will require, as a minimum, the adoption of a Code of Ethics and will recommend to the decision-making bodies in charge that they put in place suitable preventive procedures, so that it has a measure of protection against risks of administrative liability under the Decree.

3.7 The Code of Ethics of GIMA S.p.A.

The Company's Code of Ethics is viewed as a component of its Organisation, Management and Control Model; it is drawn up and adopted by the Company as a means of guiding the conduct of all those who operate on behalf of and in the interest of the company, in order to ensure the observance of standards of ethics, moral integrity and legality.

This document, which therefore forms an integral part of this Model, sets out the principles of corporate ethics and the rules of conduct that the Company recognises as its own and with which it requires compliance by all Recipients.

The Code of Ethics must be communicated to the various Recipients, in different ways depending on the type of relationship with the Company; it must be brought to the attention of Recipients in a manner that ensures that they become concretely acquainted with its provisions.

3.8 The relationship between the Organisational, Management and Control Model and the Code of Ethics

The principles and rules of conduct in this Model supplement the provisions of the Code of Ethics adopted by GIMA S.p.A., although the Model of course differs in its scope from the Code of Ethics in that it is intended primarily to implement the provisions of the Decree.

In this respect, note that:

- the ***Code of Ethics*** is an instrument of general application that the Company has adopted in order to affirm a series of principles of corporate ethics to which the Company is committed; it calls on all Recipients and stakeholders cooperating in the pursuit of corporate objectives to abide by these principles;
- the ***Model***, on the other hand, responds to the specific requirements of the Decree which are designed to prevent the commission of particular types of offence in respect of acts that, while apparently committed in the interest or for the benefit of the company, could implicate the entity in administrative liability based on the provisions of the Decree.

However, since the Code of Ethics sets out principles of conduct that are designed also to prevent the unlawful conduct referenced in the Decree, it acquires relevance in the context of the Model and therefore is seen as a formal, integral part thereof.

4. COMPONENTS OF THE ORGANISATION, MANAGEMENT AND CONTROL MODEL

4.1 Drafting of the Model

The drafting of this Model was preceded by a series of preparatory activities divided into various phases, all aimed at building a risk prevention and management system consistent with and inspired not only by the provisions of the Legislative Decree 231/01, but also by the content and suggestions based on the Confindustria Guidelines and existing best practices.
Below is a brief description of the separate phases of the task of identifying the 'areas at risk', which resulted in the drafting of this Model:

1) Phase 1 - Project planning and start-up.

In this phase, the preliminary organisation of activities was seen to and, after the team was set up and the corporate organisation comprehensively analysed, these specific activities followed - the gathering of documentation, the identification of individuals to be interviewed, the definition of the content of the interviews, and definition of business cycles.

2) Phase 2 – Risk assessment.

In this phase, interviews were carried out with representatives of the departments/functions identified in the previous phase, in order to be able to map and analyse the activities and the internal control system, and then afterwards to identify and assess the at-risk areas for each activity, and to oversee existing procedures.

The following control principles based on the Confindustria Guidelines were taken into account, among other things, when surveying the existing control system:

- existence of formalised procedures;
- traceability and *ex-post* verifiability of activities and of decisions by means of adequate supporting documentation or information;
- segregation of duties;
- existence of formalised powers of attorney/delegated powers, consistent with the organisational responsibilities conferred.

Once the control safeguards adopted for each isolated sensitive activity were identified, control standards ('protocols') were updated and, where necessary, new ones created.

3) Phase 3 – Gap analysis.

A comparative analysis was carried out between the existing procedures and a theoretical reference model assessed by reference to the content of applicable regulations, rules, best practices and case law referenced in the Legislative Decree 231/01, in order to properly assess the suitability of existing procedures to prevent and circumvent offences under the Decree.

By this comparison, it was possible to foresee areas for improvement of the existing internal control system and, based on what emerged, an Action Plan was drawn up aimed at identifying the organisational requirements characterising an organisation, management and control model that is fully in compliance with the provisions of Legislative Decree 231/2001, and at detailing the actions that could be taken to improve the internal control system in order to improve its efficacy and suitability.

4) Phase 4 – Drafting and adoption of the Model.

As part of this phase, the Model was customised to the Company's specific type of activities. The Model's completion was supported by the previous phases and by the policy choices of the company's decision-making bodies.

4.2 In particular: description of the risk analysis methodology

The management of the risk assessment process and the resulting methodology used represents a critical point in the entire process of developing an Organisational Model.

The task of identifying areas of corporate activity that could be vulnerable to the risk of commission of offenses for which entities may be held administratively liable pursuant to the Decree - i.e. the so-called Sensitive Processes - was therefore performed through a careful analysis of the Company's corporate processes and of the possible ways in which offenses might be committed, for which for the Company could be held liable.

Existing and applied operational and management practices and also existing control features were identified and analysed for each Sensitive Activity, and the figure responsible for the specific company process in question (Key Officer) was also identified, based on his or her role. A comparative analysis was carried out between the existing applied internal control system and the principles and content of the Model being drafted (in particular by analysing prevention protocols, processes and control safeguards) in order to evaluate its correct application.

Based on principal international references, the internal control system may be defined as a set of mechanisms, practices, procedures and tools implemented by company management in order to ensure the achievement of corporate efficiency objectives, while concurrently guaranteeing the reliability of corporate and financial information, compliance with laws and corporate regulations applied, the safeguarding of corporate assets and the observance of corporate business principles.
The following is a summary of the components and features of the control system that are required in order to ensure effective and proper management:

- the organisational structure;
- the allocation of authority and responsibility (including specific powers of attorney);
- integrity and respect for corporate ethical values;
- the management approach;
- policies and practices for personnel;
- the specific competences of personnel;
- policies for external suppliers and partners;
- the control systems;

- the management processes in place for handling non-compliances found;
- the proper implementation of the actions identified and measurement of their effectiveness.

4.3 Risk Assessment

In this phase, company processes were identified in which offences under the Decree were in theory vulnerable to being committed.

The identification of corporate processes and, within these, of activities vulnerable to the commission of offences was carried out through a prior examination of corporate documentation (organisation charts, service orders, procedures, powers of attorney, etc.), and by then conducting interviews and in-depth investigations with the heads of Company's Organisation Units.

Subsequently, based on the analysis of corporate processes, the potential risks were identified, i.e. the categories of offences under the Legislative Decree 231/01 which potentially applied to the Company, that could be associated with each corporate process.

4.4 As-is analysis

Once the potential risks within each process and sub-process were identified, the control system was analysed. This involved assessing the existing internal control safeguards (the procedures and/or practices adopted, the verifiability and 'traceability' - through documentation - of operations and controls, the separation or segregation of functions, the system of powers of attorney and delegated powers) by analysing information and documentation provided by the company functions during interviews or upon specific request.

4.5 Gap analysis

Based on the results obtained in the previous phase, the Company, in order to prevent the offences referenced in the Legislative Decree 231/01, identified a series of points for improvement in the internal control system, for the overcoming of which appropriate monitoring methods and actions to be taken were defined.

5. THE SYSTEM OF DELEGATED POWERS AND POWERS OF ATTORNEY

The company has, for prevention purposes, defined a system of delegated powers and powers of attorney as a way of distinguishing separate tasks and functions, thus ensuring that operations carried out are clear and traceable.

A *delegated power* is an internal act by which functions and tasks are allocated or assigned; a *power of attorney* is a unilateral transaction by which one person confers a power of representation on a third party.

In relation to the specific content of the delegated powers or powers of attorney of individual company figures:

- all persons dealing with the PA on behalf of the Company must be provided with a formal power of attorney or delegated power to that effect;
- the grant of delegated powers must associate each managerial power with the related responsibility and with a sufficiently senior position in the organisation chart, and they must be updated following organisational changes;
- each delegated power must clearly and unequivocally define the delegate's powers as well as the person to whom/which the delegate reports.

In relation specifically to powers of attorney:

- they may be granted to natural persons who are indicated in the power of attorney itself, or to legal persons who will act through their own authorised representatives who are vested with similar powers;
- general powers of attorney describe the management powers conferred and, where necessary, indicate the extent of the powers of representation and spending limits;
- special powers of attorney, on the other hand, detail the scope of operation and powers of the recipient delegatee.

In order to concretely implement Legislative Decree 231/2001, all procedures, company policies and the system of delegated powers and powers of attorney are subject to a continuous review process, which is a fundamental prerequisite for developing a system dedicated to the continuous monitoring of risk.

6. THE SUPERVISORY BODY

6.1 Introduction

Article 6(I)(b) of Legislative the Decree/2001 provides that the Entity may be exonerated from liability resulting from the commission of offenses under the Decree if the governing body has, among other things:

- adopted organisation, management and control models suitable for preventing the offenses listed;
- tasked an internal supervisory body, with independent powers of initiative and control, with overseeing the model's operation, compliance and updating (the Supervisory Body).

The entrusting of said tasks to the Supervisory Body and, obviously, the proper and effective performance of those duties are thus a necessary precondition to exemption from liability, whether the criminal offense was committed by senior managers (pursuant to Article 6 of the Decree) or by subordinate persons subject to the management or supervision of superiors (pursuant to Article 7).

6.2 Functions, composition and requirements

The Supervisory Body's allocated functions, based also on the indications contained in Articles 6 and 7 of the Decree, may be summarised as follows:

- to supervise the effectiveness of the Model, by ascertaining the extent to which actual conduct conforms to the Model's provisions;
- to examine the adequacy of the Model, i.e. of its actual (and not merely formal) ability to broadly prevent undesirable conduct;
- to analyse whether the requirements of the Model's soundness and functionality are maintained over time;
- to ensure that the Model is dynamically updated, to reflect critical analyses that indicate the necessity for corrections and adaptations.

This last activity generally occurs in two separate but mutually dependent phases:

- submission of proposals to update and adapt the Model to corporate bodies/functions that are positioned to concretely implement them within the Company. Depending on

the nature and scope of the interventions, proposals will be addressed to the Human Resources and Administration functions or to other functions or, in particularly important cases, to the Board of Directors;

- follow-up i.e. assessment of the implementation and actual operability of the solutions proposed.

The main prerequisites of the Supervisory Body are:

- independence;
- professionalism;
- continuity of action.

GIMA S.p.A. has entrusted the tasks and duties of a Supervisory Body to a multi-member monitoring agency that meets the requirements described above and is identified by the Board of Directors, subject to a prior assessment of the company's Sensitive Processes.

This *Supervisory Body (SB)*, accordingly, is tasked with implementing the supervisory and control functions provided for in this Model.

The SB, moreover, is identified according to procedures that ensure a high level of confidence that subjective eligibility requirements have been met, thus copper-fastening the independence demanded by the functions entrusted. Specifically, upon appointment, the Board of Directors receives from the designated SB a declaration confirming the absence of grounds for ineligibility and, accordingly, the presence of essential criteria such as e.g. professional integrity, absence of conflicts of interest and of close family ties with the governing bodies and with senior management.

The appointment and removal of the SB (in the latter case e.g. for the infringement of its duties under this Model) are reserved to the Board of Directors.

The SB is appointed for 3 years, renewable on each expiry date. Its appointment may be revoked exclusively for just cause.

The term "just cause" for the revocation of powers associated with the office of a SB member includes the following reasons, for purposes of illustration:

- serious non-compliance (premeditated or otherwise) with the obligations of the office (e.g. breach of trust, inefficiency, negligence, etc.);

- *'inadequate or omitted supervision'* by the SB - in accordance with the provisions of Article 6(1)(d) of the Decree - following a criminal conviction (non-appealable or otherwise) handed down against the Company pursuant to the said Decree, or following a conviction applying punishment at the request of the parties (plea-bargaining);
- supervening impossibility;
- the SB no longer meets the requirements of '*independence'* and of '*continuity of action'*;
- the SB member is an employee or director, upon termination of the employment or director's contract;
- death of am SB member or their resignation from office.

6.3 Functions, duties and powers

The SB is responsible for overseeing:

- compliance with the Model by the Company's employees and governing bodies;
- the effectiveness and adequacy of the Model in specific reference to the Company's corporate structure and its ability to prevent or avert the commission of offences under the Decree;
- the need to update the Model when it becomes clearly necessary to adapt the Model to changed corporate and/or regulatory conditions.

To this end, the SB is also entrusted with the more specific tasks of:

- proposing updates;
- proposing to the relevant corporate bodies or functions the advisability of issuing procedural provisions to implement the Model's principles and rules;
- interpreting relevant regulations with the assistance of consultants as required, and assessing whether the Model is adequate to these regulatory requirements, flagging possible areas of intervention to the Board of Directors;
- assessing the need for updating the Model, flagging possible areas of intervention to the Board of Directors;
- indicating to management any relevant additions to the systems for managing financial resources (both incoming and outgoing) that are already in place in the Company, with a view to introducing suitable mechanisms that can detect atypical financial flows characterised by greater margins of discretion than those ordinarily provided for;

- notifying the Board of Directors of the advisability of issuing special procedural provisions to implement the Model's principles, which may not be consistent with those currently in force in the company, also taking care to ensure their coordination with those that already exist;
- conducting checks and controls;
- checking compliance with company procedures put in place to safeguard Sensitive Processes within the meaning of the Model, also providing for the issuance of internal information circulars, where appropriate;
- exploring the Company's activity in general in order to update the mapping of Sensitive Processes;
- carrying out periodic targeted audits on specific operations or acts of the Company, especially in the area of Sensitive Processes, the results of which should be summarised in a special report to be submitted to the appointed corporate bodies.

Further procedures for the exercise of the SB's powers may be defined by its own internal acts or instruments, of which the Board of Directors is informed.

Moreover, in order to perform the functions entrusted to the SB, the SB is allocated, as part of the budgeting process, adequate financial, human and logistical resources consistent with the projected and reasonably achievable results.

Lastly, the SB's activities carried out in the performance of its duties are not subject to the scrutiny of any other corporate body, function or department.

With regard to the SB's functioning, more specifically, please consult the Rules approved by that body.

Information gathering.

The Supervisory Body is entrusted with the important task of gathering, processing and storing relevant information on compliance with the Model, as well as updating the list of information required to be transmitted or kept available to the SB.

Note, here, that the SB must be promptly informed by all employees - through a special internal communication channel which it establishes for this purpose - of any conduct, acts or events which could result in the Model being infringed (including reports relating to the commission,

or reasonable risk of commission, of offenses under the Legislative Decree 231/01) or which, more generally, are relevant for the purposes of that Decree. In addition to sending the SB the reports on infringements of a general nature described above, the departments and functions where Sensitive Processes take place must transmit the specific information indicated below.

Specifically, such information may concern, for example:

- decisions relating to the application for, disbursement and use of public funding;
- requests for legal assistance made by managers and/or employees against whom the judicial authorities are proceeding for offences under the Decree;
- measures and/or notices from the Criminal Investigative Police or from any other authority indicating that investigations for criminal offences are being carried out, including against persons unknown, for offences under the Decree;
- internal reports which indicate responsibility for offences under the Legislative Decree 231/01;
- information relating to the Model's effective implementation at all levels of the company, highlighting any disciplinary proceedings and any penalties imposed, or the dismissal of such proceedings and the associated reasons.

The SB also coordinates with the other company functions in order to optimally oversee activities based on the procedures established in the Model.

To this end, the SB has free access to all company documentation which it considers relevant, and management must keep it continuously informed:

- about aspects of the Company's activities that could expose the Company to the risk of commission of a predicate offense;
- about relationships with Consultants and with Partners who operate on the Company's behalf in the context of Sensitive Processes.

The SB may also conduct internal investigations, liaising from time to time with the relevant corporate functions to obtain additional material for investigation.

Training.

In this specific area, the Supervisory Body may carry out the following activities:

- coordinating with the Personnel Manager in order to define staff training programs and the content of periodic communications destined for employees and the corporate bodies, aimed to adequately acquaint and familiarise them with the Decree's provisions;
- regularly ascertaining the quality of such training programs, once defined;
- overseeing initiatives to promote knowledge and understanding of the Model and drafting the internal documentation necessary for its effective implementation, containing instructions for use, clarifications or updates thereto.

Infringements and sanctions.

In this specific area, the Supervisory Body may carry out the following activities:

- reporting any infringements of the Model and of the Decree to the relevant corporate function, to the Board of Directors and to the Personnel Manager;
- coordinating with the Board of Directors and with the Personnel Manager in order to assess the merits of adopting any disciplinary sanctions, without prejudice to the latter's competence to impose a sanction and implement the corresponding disciplinary procedure;
- indicating the most appropriate measures to remedy infringements.

General provision.

By reason of the tasks entrusted, the Board of Directors is tasked as the sole corporate body with remit to oversee the adequacy of the Supervisory Body's actions or interventions, as the ultimate responsibility for the operation and effectiveness of the Model rests with the management body.

The SB, without prejudice to any other prevailing provision of law applicable, enjoys free and unrestricted access (without the need to obtain prior consent) to all Company functions in order to gather any information and data required to enable it to fulfil its responsibilities under the Legislative Decree 231/01.

The independence that is demanded by the SB's activities has made it necessary to introduce various ways to safeguard its status, in order to guarantee the effectiveness of the Model and to make sure that the SB's supervisory role does not generate forms of retaliation against it (for example, cases in which the SB's investigative activities reveal evidence that links the offense or attempted offense or infringement of this Model to the company's senior management).

Accordingly, decisions about remuneration, promotions, transfers, or disciplinary sanctions involving SB members are within the exclusive remit of the Board of Directors.

6.4 The Supervisory Body's Information flows: its reports to senior management

The SB reports on the implementation of the Model, and on any critical issues that arise.

More specifically, it has two lines of reporting activity:

- the first is an *ongoing* direct reporting line to the legal representative (Managing Director);
- the second is an *annual* reporting line to the Board of Directors and the Board of Statutory Auditors.

In particular, the SB prepares a written report for the Board of Directors and the Board of Statutory Auditors on the activity carried out (indicating the controls and checks carried out and their results, any specific checks and their results and any updates to the mapping of Sensitive Processes, specifying the statement of account of the fund managed by it, etc.). If the SB should detect critical issues referable to any of the reporting parties, the corresponding report must be promptly addressed to the Directors and Auditors.

More specifically, the reporting activity relates to:

- the services performed by the SB's office;
- any critical issues (and suggestions for improvement) that have emerged in terms of conduct or events occurring within the Company or in terms of the Model's efficacy.

Meetings with the bodies to which the SB reports must be recorded, and copies of the minutes must be kept by the SB and by the governing bodies involved from time to time. The Board of Directors, the Chairperson and the Board of Statutory Auditors have authority to convene the SB at any time. Likewise, the SB has authority to request, through the competent functions or individuals, the convening/summoning of said governing bodies, if the reasons are urgent.

The SB must also coordinate with the Company's competent functions, based on the various roles involved, i.e.:

- with the *Personnel Manager*, for personnel training;
- with the *Personnel Manager*, for disciplinary proceedings;

- with the *Administrative Manager*, for the control of financial flows and for any activities, including administrative activities, relevant to the commission of corporate offenses;
- with the *Employer*, for accident prevention and health and hygiene protection activities and also for activities related to environmental regulations.

6.5 Information flows to the Supervisory Body: general information and specific mandatory information

Article 6(II)(d) of the Legislative Decree 231/01, requires the company Model to provide for reporting obligations to the body that is appointed to oversee the operation and observance of the Model (i.e. the Supervisory Body). The obligation to ensure a properly structured information flow was devised as a way of ensuring that the Model's effectiveness could be properly supervised, and to facilitate any retrospective assessment of the causes that enabled offences under the Decree to be committed in the past.

The effectiveness of the SB's supervisory activities is based on a structured system of reporting and information originating from all of the Model's Recipients, related to acts, conduct, events or circumstances that come to their attention which may infringe the Model or are, more generally, of interest for the purposes of the Decree.

As provided for by the Confindustria Guidelines and by best practice in the sector, information flows to the SB refer to the following categories of information:

- ad hoc information flows (concerning actual or potential critical concerns that should be immediately reported to the SB, as indicated in greater detail in para. 6.5.1 below);
- periodic reporting (on multiple and diverse aspects which the SB should be informed about at predetermined intervals – typically annually or half-yearly – to facilitate the monitoring of compliance with the rules of conduct set out in the individual Special Parts of the Model, as further explained below in para. 6.5.2 and in the summary tables at the end of each Special Part).

6.5.1. Ad hoc information flows

Ad hoc information flows to the SB from key corporate officers or from third parties involve actual or potential critical issues and may involve:

occasional information that needs to be immediately reported to the SB.

The following types of information must be reported to the SB:

- official measures and/or information from the judicial authorities or from any other authority, which reveal that investigations/inquiries are being carried out concerning the Company for criminal/administrative offences pursuant to the Decree, also against persons unknown;
- requests for legal assistance submitted by managers and/or employees, in the event that legal proceedings are instituted for offences pursuant to the Decree;
- information on the activation, at all corporate levels, of the disciplinary system provided for in the Model, with specific details of any disciplinary proceedings initiated and any sanctions imposed, or of the dismissal of such proceedings, indicating the reasons;
- reports revealing evidence that raises critical concerns in terms of compliance with the Decree's provisions;
- potential conflicts of interest between any Recipient and the Company;
- any workplace accidents with a prognosis of 40 days or more, or measures taken by the Judicial Authorities or other authorities in the workplace health and safety field;
- any incidents or events that may pose an environmental risk;
- any violations of the GDPR or data breaches.

The SB evaluates the information flows received and decides what initiatives should be taken, if any, also giving the reporting party and/or alleged perpetrator and/or any other potentially useful party the opportunity to be heard, justifying in writing any conclusions reached.

6.5.2. Periodic reporting

In addition to the information referenced above – which concern exceptional facts or events – the SB must also receive relevant information on a periodic basis to facilitate its monitoring activity, as outlined in the summary tables at the end of each Special Part.

6.5.3. E-mail box and address of the Supervisory Body

The SB's e-mail box has been set up to order to facilitate the reporting and information flow: odv@gimaitaly.com, which has been communicated to Recipients.

Information flows may also be transmitted by post to the address: *Organismo di Vigilanza* ex *D.Lgs. n. 231/2001, via Marconi n. 1, Gessate (MI).*

The SB may also request the auditing firm for information of interest for the purposes of implementing the Model and monitoring compliance therewith.

The SB ensures the confidentiality of the information it comes into possession of.

The SB also refrains from using confidential information for purposes other than those outlined in the previous paragraphs or for purposes inconsistent with the functions of a supervisory body, except in cases of explicit and informed authorisation.

6.6. Collection and storage of information

The Supervisory Body is obliged to store any information or report provided for by this Model in a dedicated digital or print archive/database for a period of 10 years, in compliance with applicable data protection regulations (Legislative Decree 196/2003 and EU Regulation 679/2016).
Only the Board of Statutory Auditors and the Board of Directors are entitled to access this archive/database, unless the information concerns investigations involving them, in which case authorisation from the Board of Directors is required, following consultation with the Board of Statutory Auditors, and provided that such access is not otherwise guaranteed by applicable laws.

7. WHISTLEBLOWER PROTECTION

Legislative Decree no. 24 of 10 March 2023 - transposing Directive (EU) 2019/1937 into the national law of our country - replaced the earlier provisions on whistleblowing and brought together in a single text the entire regulatory system of communication channels and protection measures for persons reporting violations of national or EU regulations that harm the public

interest or the integrity of a private entity (or that of the public administration), of which they have become aware in their own working environment.

In order to ensure effective implementation of the provisions set out in Legislative Decree 24/2023, which, among other things, abrogated the provisions laid down in article 6, paragraph 2-ter and paragraph 2-quater, and amended article 6, paragraph 2-bis, of Decree 231, GIMA S.P.A. has adopted a new "Whistleblowing Procedure" that constitutes an integral part of the Model 231 adopted (annexed hereto) and governs the receipt, analysis and management modalities of whistleblowing reports.

In particular, the Whistleblowing Procedure:

- provides for communication channels that enable anyone to submit reports on violations of laws (including European ones), regulations, Codes of Ethics, Model 231 provisions, and company systems of rules and procedures;
- ensures, also through the use of encryption tools, the confidentiality of the identity of the whistleblower and the people involved in the report, as well as the confidentiality of the content of the report itself and the relevant documentation;
- provides for measures protecting those who submit a report, who disclose the information to the public or who report the violation to the judicial or the accounting authorities, as well as measures protecting the other parties specifically identified by Legislative Decree 24/2023 (e.g., facilitators, colleagues, etc.);
- prohibits any form of retaliation against those who submit a report, disclose the information to the public, or report the violation to the judicial or the accounting authorities, as well as against the other parties specifically identified by Legislative Decree 24/2023 (e.g., facilitators, colleagues, etc.);

In compliance with Article 6, paragraph 2-bis, of Decree 231 and Legislative Decree 24/2023, the Model extends the scope of application of the sanctions as per the Disciplinary System to anyone who breaches the rules on the management of the reports and/or the measures put in place to protect the whistleblowers, as well as to the whistleblowers themselves in the cases contemplated in Article 16(3) of Legislative Decree 24/2023, except for the cases described in article 21, paragraph 1, letter c), of Legislative Decree 24/2023 (see below paragraph 11 of the Disciplinary System).

Reports can be submitted:

In written form:

- ✓ through the Web Portal accessible from the Whistleblowing page that can be found both on the GIMA S.P.A. website and on the company intranet https://www.gimaitaly.com/it/assets/Procedura_Whistleblowing.pdf

Verbally:

- ✓ by voice mail

Reports may also be submitted:

- verbally, by requesting a face-to-face meeting;
- through the external channel managed by ANAC;
- through a report to the judicial authorities;
- through public disclosure.

The internal channel takes priority over the external one.

For more information on what is addressed in this section, see the Whistleblowing Procedure.

8. GENERAL DATA PROTECTION REGULATION

One of the main regulatory innovations introduced in 2018, having a decisive impact on company procedures, was the new European data protection regulation, Regulation (EU) 2016/679 (known as the General Data Protection Regulation - GDPR), which must necessarily be complied with by all addressees, such as companies, private and public bodies, and professionals who have a duty to ensure maximum compliance with the regulations on confidentiality and personal data protection.

The GDPR applies to all companies that collect and/or process the personal data of European citizens, even companies holding the data which are based outside the boundaries of the EU but offer services and/or products within the single market.

The GDPR applies to all companies, irrespective of where they are located, so as to offer direct protection to EU citizens by requiring companies to comply with the new provisions.

Compared to the earlier regulations, the GDPR introduced detailed requirements that made it possible to complete and implement the data processing and protection system previously adopted by the parties required to do so. In particular, the rules provided for can be summarised as follows:

- define a data retention policy;
- update the notices pursuant to article 13 of the GDPR;
- verify the legitimacy of processing modalities and assess the circumstances in which consent has to be requested (articles from 6 to 10);
- revise the relationships with external processors (repealing the obligations provided for in article 28);
- revise/update the risk analysis for the definition of adequate security measures (article 32);
- require public bodies (and private bodies, if the conditions described in article 37, paragraph 1, apply) to identify and appoint a Data Protection Officer (DPO).

The GDPR widened the definition of personal and sensitive data to beyond data such as addresses and telephone numbers to include online identity data such as cookies, IP addresses, geolocation and email data.

To comply with the new regulation, when collecting data, all companies must abide by the following requirements:

- enable users to give their consent in an explicit and traceable manner;
- provide transparent, clear and readily accessible notices on the processing of personal data;
- make sure that the data collected are relevant, suitable and limited to the purposes for which they were originally requested and processed.

The request for consent must be clear, understandable and presented in an easily recognisable screen. Users should also be guaranteed the right to revoke their consent at any time.

The GDPR introduces the right to the “portability” of one's personal data, i.e., the possibility for any user to transfer their personal data from one data controller to another. Data subjects must be able to easily obtain a copy of their personal data in a readable and easily transferable format.

The obligations of the Data Controller and the Data Processor have been extended (articles 24 et seq.).

Besides ensuring compliance with the rules governing the processing of personal data, they have to put in place a number of juridical, organisational and technical measures for the protection of personal data, including through the preparation of specific organisational models for the sectors in which they operate.

Any data breach must be notified to the supervisory authorities by the Data Controller and any delay or failure to do so exposes the latter to administrative sanctions.

Among the main obligations to be complied with is the requirement to create and maintain Records of Processing Activities (articles 30).

The Data Controller is also required to inform all the data subjects concerned in a clear, simple and direct manner, as well as to tell them how it intends to limit the damage. It may decide not to inform the subjects concerned if it deems that the breach does not entail a high risk for their rights, it can prove that it has already taken security measures, and if informing the data subjects would entail an effort disproportionate to the risk entailed.

The Supervisory Authority may require the Data Controller to inform the data subjects on the basis of its own assessment of the risks entailed by the breach.

Following the transposition of the GDPR, the company put in place new measures in keeping with the new requirements.

9. THE DISCIPLINARY AND SANCTIONS SYSTEM

9.1 General Principles

For the effective implementation of organisation, management, and control models, the Legislative Decree 231/01 requires the establishment of a suitable Disciplinary System (Article 6 (II)(e) and Article 7 (IV)(b) of the Decree).

The Disciplinary System adopted by GIMA S.p.A. is aimed at sanctioning non-compliance with the principles, measures, and rules of conduct set out in the Model and also in the associated procedures, including the Whistleblowing Procedure.

Disciplinary sanctions are applied irrespective of whether the conduct attributed to the worker (whether subordinate, senior, or a collaborator) represents a breach of the law that results or could result in criminal proceedings and/or the application of sanctions of a different kind.

The Disciplinary System adopted by the Company is consistent with the following principles:

- **Specificity and autonomy**: The Disciplinary System is designed to sanction any infringement of the Model, regardless of whether it involves the commission of an offence. The Disciplinary System thus represents an independent regime of sanctions separate from other sanctions regimes, since the Company is required to punish infringements of the Model independently of any criminal proceedings and their outcome.
- **Compatibility**: the procedure for ascertaining and applying sanctions must be consistent with applicable laws and contractual rules governing the relationship with the Company.
- **Suitability**: The system must be efficient and effective in preventing the risk of offences being committed, with particular reference to conduct that is relevant to the commission of offences under the Decree.
- **Proportionality**: The sanction must be proportionate to the violation identified. Proportionality is assessed based on two criteria: (i) the severity of the infringement and (ii) the type of employment relationship (subordinate employment, quasi self-employment, executive, etc.), taking into account the specific legal and contractual framework;

- **Written formalisation and adequate dissemination:** the Disciplinary System must be formalised in writing and must be the subject of specific information and training provision for all Recipients.

Compliance with the provisions of the Model is required under both independent self-employment contracts (including coordinated and continuous contracts and/or outsourced contracts) and subordinate employment contracts, with the latter being subject to the applicable disciplinary sanction's framework (Article 7 of Law no. 300 of 20 May 1970, the so-called "Workers' Statute" and the applicable National Collective Labour Agreement).

The Supervisory Body, with the support of the HRO Function, is responsible for monitoring the functioning and effectiveness of the Disciplinary System.

The disciplinary process is initiated either by the HRO Function or following a communication from the SB of non-compliance and/or potential infringement of the Model, sent to the relevant functions.

In cases where, as further outlined below, the SB does not conduct the investigation into potential non-compliance and/or infringements of the Model, the SB serves in an advisory capacity. In all cases, the SB also provides advisory input in the disciplinary process of imposing sanctions.

Specifically, the SB must be informed in advance of any proposal to close a disciplinary proceeding or to impose a disciplinary sanction for an infringement of the Model so that it may, if necessary, express its opinion. The SB's opinion must be provided by the deadline set for the conclusion of the disciplinary proceeding.

The conduct and resolution of disciplinary proceeding are entrusted, depending on the type of employment contract and/or role involved, to the governing bodies and/or to Company functions duly authorised under of the powers and responsibilities conferred on them by applicable laws, by the Company's Articles of Association, and by internal rules.

The Company reserves the right to seek compensation for any loss and/or liability that may result from the actions of employees, members of governing bodies or Third Parties in violation of the Model.

The Disciplinary System adopted by GIMA S.p.A. is consistent with applicable laws and other regulatory provisions, and with the relevant National Collective Labour Agreements for the sector. With regard to the application of sanctions in the context of subordinate employment relationships, the Disciplinary System also complies with Article 7 of the Workers' Statute.

For Recipients who are bound by contracts other than subordinate employment contracts (including the members of governing bodies and Third Parties in general), the applicable measures and disciplinary procedures must comply with law and with the relevant contractual terms.

9.2 Recipients

Recipients are obliged to conform their conduct to the principles and rules laid down in the Organisation Model.

For the purposes of the Disciplinary System, any action or omission - including in combination with other parties - that violates the aforementioned principles and rules represents relevant conduct for the application of sanctions.

Below are specific examples of disciplinary offences, beyond what is provided in the relevant in-house rules (and as a specification thereof):

- the non-observance or violation of the ethical rules of conduct provided for by the Organisation Model;
- the failure to report to the Supervisory Body infringements of the Model that have come to one’s attention;
- retaliation i.e. any conduct or act or omission, even if only attempted or threatened, resulting from a whistleblowing report, or from a formal complaint filed with the judicial or accounting authorities or from a public disclosure, which causes or could cause (directly or indirectly) unjust harm to the reporting party or to the person who filed the complaint or who made a public disclosure, and/or to the other persons identified under Legislative Decree 24/2023;
- the failure to establish internal reporting channels;
- the failure to adopt procedures for making and managing reports;

- the adoption of procedures for making and managing reports that do not comply with the requirements of Articles 4 and 5 of Legislative Decree 24/2023;
- the failure to verify and examine reports received;
- any actions or conduct that hinder or attempt to hinder or obstruct a report;
- violation of the obligation to keep confidential the identity of the whistleblower and of those who are involved or who are (as applicable) mentioned in the report, and also to keep confidential the content of the report and the related documentation.

In the cases referred to in Article 16, paragraph III, of Legislative Decree 24/2023 (i.e. where a court - including a first instance court in a non-final judgment - holds a whistleblower criminally liable for the offences of slander or defamation or for the same offences involved in the complaint to the judicial or accounting authorities, or holds the whistleblower civilly liable for having provided false information reported with deliberate intent or gross negligence), except as provided for in Article 21, paragraph I, letter c) of Legislative Decree 24/2023, the Company will initiate disciplinary proceedings in conformity with law, and in accordance with the provisions of the Disciplinary System, of the National Collective Labour Agreement for Telecommunications (*CCNL TLC*) and of applicable laws.

Any conduct in breach of the provisions of the Organisation Model shall - if ascertained:

- in the case of employees (including managers), constitute a breach of contract based on the infringement of obligations arising from the employment relationship pursuant to Articles 2104 and 2106 of the Italian Civil Code;
- in the case of Directors and members of the Board of Statutory Auditors, constitute a failure to comply with the duties imposed on them by law and/or by the articles of association;
- in the case of Third Parties, constitute a serious breach of contract granting entitlement, in the most serious cases, to terminate the contract pursuant to Article 1456 of the Italian Civil Code, without prejudice to the right to seek compensation for any loss incurred.

The procedure for the imposition of disciplinary sanctions thus takes into account specific aspects deriving from the legal status of the person against whom the proceedings are brought.

9.3 Sanctions against employees

9.3.1 Measures against office workers and middle managers.

The infringement of the rules of conduct and procedures indicated in the Model constitutes a disciplinary offence, pursuant to Article 2104, para. II of the Italian Civil Code.
More specifically, it is provided that:

- a worker will receive a verbal caution, a written caution, a fine or suspension from work and pay, depending on the seriousness of the infringement, if he/she infringes the Model's internal procedures (e.g. by failing to comply with the prescribed procedures, or to inform the Supervisory Body of the prescribed information, or to carry out checks, etc.), or engages in acts/conduct inconsistent with the Model's provisions while operating in the relevant at-risk areas, as such conduct represents a breach of contract undermining the Company's disciplinary ethic and morale;
- furthermore, a worker who commits a more serious violation of the Model's provisions while operating in areas deemed vulnerable to the risk of commission of offences, shall also be subject to dismissal with notice. Such conduct is considered a more serious violation than that outlined in the previous point;
- finally a worker shall also be subject to dismissal without notice if he or she, while operating in at-risk areas, acts in a manner unequivocally intended to commit an offence under the Decree or in violation of the Organisation Model, thereby exposing the Company to concrete penalties under the Decree. Such behaviour is considered a very serious violation that causes "serious moral and/or material harm to the Company" and also constitutes a "criminal offence".

These sanctions may also be imposed for conduct identified as infringements under the Whistleblowing Decree.

9.3.2 Measures against managers.

In the event that managers infringe this Model or engage in conduct incompatible with the Model's provisions while performing Sensitive Processes, or if the measures protecting whistleblowers are infringed in any way, or if reports are submitted, negligently or with fraudulent intent, that later prove unfounded, the Company will take the most appropriate measures against those responsible, in accordance with applicable regulatory provisions and in conformity with the National Collective Labour Agreement for Industry Managers.

The identification and application of sanctions must be based on the following principles: the sanctions must be proportionate, progressive and commensurate with the infringement alleged. The following circumstances are of relevance in this context:

- the nature of the alleged conduct;
- the specific circumstances in which the conduct occurred;
- the manner in which the offence was committed;
- the severity of the violation, taking into account the following subjective elements:
    - the possible commission of multiple infringements from the same conduct;
    - the possible sharing of responsibility with multiple parties who were complicit in the violation;
    - possible repeat offences;
    - the level of hierarchical or technical responsibility attributable to the perpetrator;
- the objective severity of the violation, taking into account the following three elements, ranked in progressive order:
    - violations of the Model that did not produce an exposure to risk or that produced minimal exposure to risk;
    - violations of the Model that resulted in appreciable or significant exposure to risk;
    - violations of the Model that constituted a criminal offence.

In particular:

- if the violation of one or more provisions of the Model is of such severity as to irreparably damage the relationship of trust, making even the temporary continuation of the employment relationship impossible, the manager shall be subject to dismissal without notice;
- in the event of a less serious violation of one or more provisions of the Model, which is still of such severity as to irreparably damage the relationship of trust, the manager shall be subject to justified dismissal with notice;
- in the event of a minor violation of one or more rules of procedure or conduct provided for in the Model, the manager shall receive a written caution and warning to comply with the Model, which is a necessary condition for maintaining the relationship of trust with the Company, as well as a fine.

These sanctions may also be imposed for conduct identified as infringements under the Whistleblowing Decree.

9.4 Procedure for determining and imposing sanctions on employees

The process for identifying infringements by employees (including office staff, middle managers and managers) and for determining and imposing sanctions is governed by applicable legal provisions and collective labour agreements. It is structured into the following three phases:

i. Investigative phase;
ii. Formal notification of the infringement to the person concerned;
iii. Determination and imposition of the sanction.

The infringement is determined through an investigation conducted by the Supervisory Body. More specifically, the SB must act whenever it receives a report or acquires information during the course of its supervisory and verification activities, suggesting a potential violation of the Model: it must carry out the necessary checks, inspections and controls that are within its remit. Once the verification process is completed, the SB, based on the information in its possession, evaluates whether a violation has occurred and informs the senior management thereof. This evaluation is formalised in a report containing the following information:

- particulars of the person responsible for the infringement;
- description of the alleged misconduct;
- reference to the provisions of the Model that have been infringed;
- any supporting documents or evidence for the allegation.

9.4.1 Procedure to be followed against office staff and middle managers.

If the provisions of the Model and Code of Ethics should be infringed by employees, the SB's report is forwarded to the HR Department. Within ten days of receiving the report, the HR Department will send the employee a written notice of the alleged infringement, including:

- specific details of the alleged misconduct;
- the provisions of the Model that have been infringed;
- notice of the right to submit written defences and/or justifications within five days of receiving the notice, as well as the right to request the involvement of the representative of the trade union to which the employee belongs or has granted a mandate.

Following any counter-arguments from the employee, the HR Department will determine the extent of the measures to be taken regarding the application of the sanction. If no sanction is

imposed within 30 days of receiving the justifications, the justifications will be deemed accepted.

The decision taken is also notified to the SB, which verifies the actual application of the imposed sanction.

The employee, while retaining the right to appeal to the Judicial Authority, may, within 20 days of receiving the decision, initiate a hearing before a Conciliation and Arbitration Board. In such a case, the sanction will be suspended until the Board's decision.

Throughout the above process, the Board of Directors of GIMA S.p.A. is informed of the outcomes of internal investigations and of the sanctions that are applied to employees.

9.4.2 Procedure to be followed against managers.

In the event that a manger infringes the Model and the Code of Ethics, the aforementioned Supervisory Body report is forwarded to the directors and to the HR Department.

Within five days of receiving the SB's report, the Managing Director summons the manager in question by issuing a written notice of complaint, which includes:

- details of the conduct alleged and the provisions of the Model allegedly infringed;
- notice of the date of the hearing and the right of the individual concerned to submit written or verbal statements on the facts, also during the hearing itself.

After this, the Managing Director and/or the Board of Directors, in consultation with the HR Department, will determine the position of the individual and implement the relevant disciplinary procedure.

If the individual subject to the formal complaint procedure holds a senior management position with delegated authority from the directors, and if the investigation confirms their involvement under the Decree, the following applies:

- the directors may decide to revoke the delegated powers granted, depending upon the nature of the role;
- the directors may take steps to determine the individual's position and implement the relevant disciplinary procedure.

The measure imposing the sanction shall be notified in writing to the person concerned, within six days of receipt of the manager's justifications. This period shall run from the date on which the written justifications or, if later, the oral justifications were provided.

The Human Resources Department formally notifies the SB of any sanctions imposed. The SB checks the documentation confirming the actual application of the sanction.

Without prejudice to the manager's entitlement to bring an action before the courts, the manager may, within 30 days of receiving written notice of dismissal, refer the matter to the Conciliation and Arbitration Board in conformity with the procedures provided for by the national collective labour agreement in force.

If the Board is appointed, the disciplinary sanction is suspended until the Board issues its decision.

9.5 Disciplinary measures and related procedure against directors and auditors

In the event that one or more directors and/or the auditor infringes the provisions of the Model and Code of Ethics and/or commits significant breaches of the Whistleblowing Decree, the SB shall inform the governing bodies. These bodies, within their respective competences, will take the most appropriate and adequate actions in line with the severity of the infringement and in accordance with their legal powers (e.g. recording statements in meeting minutes, issuing formal warnings, reducing remunerations or fees, revoking appointments, etc.).

If infringements of the Model by directors are identified that compromise the relationship of trust with the company representative, or if grave reasons exist to safeguard the company's interests and/or reputation (e.g. by seeking interim measures against the director, or committing him/her to trial for offences that could result in administrative liability for the company), the Board of Directors will be convened to decide on the revocation of the director's mandate.

In all other cases, the following sanctions may be applied:

- written caution;
- monetary penalty, amounting to two to five times the monthly pay;
- total or partial revocation of powers of attorney and/or delegated powers.

For violations of the Model that did not result in exposure to risk or resulted in minimal exposure to risk, a written caution may be issued.

For violations of the Model that resulted in appreciable or significant exposure to risk, a monetary penalty and/or total or partial revocation of powers of attorney and/or delegated powers may be imposed.

For violations of the Model that constitute a criminal offence, the appointment will be revoked.

9.6 Disciplinary measures and related procedure against collaborators, auditors, consultants, partners, counterparties and other third parties

Any conduct by collaborators, auditors, consultants, partners, counterparties and other third parties in conflict with the lines of conduct indicated in this Model and Code of Ethics may lead

to the termination of the contractual relationship, through the activation of specific contractual clauses.

To facilitate the adoption of the initiatives provided for by the contractual clauses indicated, the Supervisory Body, after the preliminary investigation phase, shall forward the report referenced in the preceding paragraph to the head of the Department/Function or Organisation Unit that manages the contractual relationship, and also to the Chairperson of the Board of Directors and/or the Managing Director.

If the contract was approved by the Board of Directors, the aforementioned report must also be brought to the attention of the Board and the Board of Statutory Auditors.

The Head of the Department/Function or Organisational Unit managing the contractual relationship, based on any decisions adopted in the meantime by the Board of Directors and/or Managing Director and by the Board of Statutory Auditors in the prescribed cases, sends the individual concerned a written communication indicating: details of the alleged conduct; the provisions of the Model that have been infringed; the specific contractual clauses whose application is requested.

9.7 *Disciplinary measures against the Supervisory Body*

In the event that one or more members of the Supervisory Body should infringe this Model and/or the provisions of the Whistleblowing Decree, the other members of the SB or any Auditor or Director shall immediately inform the Board of Statutory Auditors and the Board of Directors of the occurrence.

The Board of Directors will then take appropriate measures, including, for example: revoking the appointment of the SB members who violated the Model and appointing new members to replace them, or revoking the appointment of the entire SB and appointing a new Supervisory Body.

9.8 Whistleblowing Measures

GIMA S.p.A. does not tolerate threats or retaliation of any kind against whistleblowers or those who have collaborated in verifying the validity of a report. The company reserves the right to take appropriate action against anyone who engages in or threatens to engage in retaliatory acts against those who have submitted reports under this Model or, more generally, under the whistleblowing policy.

Sanctions against individuals who make malicious or grossly negligent reports that prove to be unfounded are included among the measures outlined in the preceding paragraphs.

10. TRAINING OF HUMAN RESOURCES AND DISSEMINATION OF THE MODEL

10.1 Training provision

Training is an essential tool for the effective implementation of the Model and for the widespread dissemination of the conduct and control principles and standards adopted by GIMA S.p.A. to ensure reasonable prevention of offences under the Decree.

Training/information on whistleblowing is also included within the Company's training plans.

Training must meet the following prerequisites:

- it must be appropriate to the position held and to the level of responsibility of individuals within the organisation (senior managers, subordinate persons, new recruits, employees, managers etc.);
- the content of the training must be differentiated based on the individual's role within the company and that individual's risk profile for offences under the Decree;
- the frequency of training activities must be determined on the basis of regulatory updates to Legislative Decree 231 and the significance of organisational changes adopted by the Company;
- participation in the training program must be mandatory, and specific control mechanisms must be established in order to verify attendance and the level of learning of each participant.

To support the adoption of the Model, the Company ensures that all employees receive training modules, activities, and projects on Decree 231-related topics based on the following principles:

- targeted training to improve and update the Decree 231-related competencies that are associated with the corporate roles most involved, and training on the responsibilities defined pursuant to the Model;
- general training targeted towards broad segments of the company population;
- special onboarding initiatives for newly recruited employees following their recruitment.

The training activities, for which specific annual planning is envisaged, are implemented by:

- liaison between Compliance functions and those responsible for training within the HR Function, while training initiatives are being devised, planned and delivered;
- tracking of all training initiatives implemented, which is also ensured by specific reporting and support systems of the HR Function.

The failure by key corporate officers to participate in training activities without justification is an infringement of the principles contained in this Model and may therefore be subject to sanctions as outlined in the previous Chapter.

10.2 Information provision

In line with the provisions of the Decree and the Confindustria Guidelines, the Company promotes adequate dissemination of this Model, in order to ensure its full understanding by Recipients.

More specifically, it is provided that:

- communication be performed through appropriate and easily accessible channels for both employees and Third Parties, such as the company's intranet portal and website;
- communication be differentiated in content by reference to the various Recipients, and timely in order to facilitate updates.

GIMA S.p.A. also implements familiarisation activities related to business ethics for third parties in the context of their business dealings with the Company. This is achieved through the inclusion of specific contractual clauses that require these parties to explicitly commit to complying with Legislative Decree 231 and to adhere to the ethical rules of conduct set out in the Model. In the most serious cases, failure to comply may result in the automatic termination of the contract under Article 1456 of the Italian Civil Code.

SPECIAL PART

INTRODUCTION TO THE SPECIAL PART

Article 6, paragraph I, of Legislative Decree 231/2001 identifies the requirements that the Organisational and Control Model must meet. Specifically, organisation models can provide exemption from administrative liability under the Decree if:

a) the governing body has adopted and effectively implemented, prior to the commission of the offense, organisation and management models suitable for preventing offenses of the type that occurred;

b) an internal supervisory body with independent powers of initiative and control has been tasked with overseeing the operation of and compliance with the models, and updating them;

c) the perpetrators committed the offense by fraudulently circumventing organisational models in place;

d) the supervisory body referenced in letter b) did not fail in its supervisory duties, either by omission or inadequate oversight.

In identifying applicable procedures, this Model has set out a series of principles that must be observed in the conduct of all activities by the Company.

Specifically, the following must be ensured:

- clear and structured distribution of tasks within the Company;
- traceability of every operation relevant to the Legislative Decree 231/2001;
- a constant flow of relevant information to the Supervisory Body.

The provisions of this Special Part of the Model apply to persons included in the company's organisational chart and operating in risk areas, as identified below in relation to each offense category described.

Recipients of the Model must absolutely refrain from:

- conduct that constitutes a criminal offense under the Special Part;
- conduct that, while not constituting offences per se, could potentially lead to such offences.

SPECIAL PART - A -

Offences in dealings with the Public Administration (PA) and inducement not to make statements, or to make false statements to the judicial authorities.

CHAPTER A.1

Criteria for defining public administration, public officials and public service officers.

The offences covered in this Special Part all presuppose the establishment of relations with the Public Administration (PA), including the PA of foreign States.

Below are some general criteria for defining *"public administration", "public officials"* and *"public service officers"*.

A.1.1 *Public Administration Entities*

For the purposes of criminal law, any legal entity that deals with public interests and carries out legislative, judicial, or administrative activities under public law rules, and acts of public authority, is generally considered to be a Public Administration body (PA body).

For example, the following entities or categories of entities may be considered to be PA bodies:

- independently operating State entities and administrations (e.g. Ministries, Parliament, Italian Tax Authority, judges of the ordinary and administrative courts);
- the Regions and Municipalities;
- municipal companies;
- contracting authorities;
- the National Institute of Health (ISS);
- hospital entities;
- supervisory authorities (e.g. Bank of Italy, CONSOB, the Italian Competition Authority (AGCM));
- Chambers of Commerce and their respective associations;

- all national, regional and local not-for-profit public bodies - e.g. National Social Security Institute (INPS), National Research Council (CNR), National Institute for Insurance against Occupational Accidents (INAIL), National Statistics Institute (ISTAT), Italian support body for Sales Representatives and Agents (ENASARCO);
- Local Health Authority (ASL) and Health Protection Agency (ATS);
- entities and monopolies of the State;
- private law entities providing public services - e.g. Cassa Depositi e Prestiti (Bank for Deposits and Loans) and the Italian State Railways;
- social security and welfare foundations;
- the Italian Society of Authors and Publishers (SIAE);
- the customs authorities;
- the Labour Inspectorate.

While this list is purely illustrative, it is important to note that not all individuals acting within or in relation to these entities are subjects against whom (or by whom) offences in dealings with the PA are committed.

The relevant figures for this purpose are exclusively *"public officials"* and *"public service officers"*.

A.1.2 *Public officials*

Article 357 of the Italian Penal Code defines public officials as "*those who exercise a public legislative, judicial or administrative function*," specifying that *"a public administrative function is one regulated by public law rules and acts of public authority, characterised by the formation and manifestation of the will of the public administration or its exercise through certification or authorisation powers"*.

The Penal Code provides for three types of public functions: legislative, judicial, and administrative.

Article 357 of the Penal Code does not explicitly define the first two (legislative and judicial) because they have typical characteristics that permit their immediate identification:

- the legislative function is implemented by public bodies (Parliament, Regions and Government) which, under the Italian Constitution, have the power to issue acts having the force of law;
- the judicial function is performed by judicial bodies (civil, criminal and administrative) and their assistants (court clerk, secretary, court technical expert, interpreter, etc.), for the application of the law to the specific case.

The administrative function, as defined by Article 357(2) of the Penal Code, is notable in that it is governed by public law rules or by acts of public authority of the PA (and this differentiates it from private law activities that are governed by instruments of private law, such as contracts) and by the fact that it is accompanied by at least one of the following three powers:

- the power to form and manifest the will of the PA (e.g. the Mayor or a councillor of a municipality, members of tender adjudication committees, managers of public companies, etc.);
- the authorisation power by which the PA's relationship of authority vis-a-vis private citizens is manifested (e.g. members of the police force, inspection committees for works done for a public body, officials of supervisory authorities, etc.);
- the certification power by which documents are drawn up, to which the legal system attributes privileged probative value (e.g. notaries).

For the purposes of determining the status of "*public official*", the Supreme Court of Cassation has ruled (in judgment no. 31676 of 28 June 2017, Division V) that one must always assess the "*specific job duties performed*" by the person where these are "*typically public functions*". This was so in this case, where the Court held that the *project manager* of a company in which a public entity has a stake was a public official).

A.1.3 *Public service officer*

The definition of the category of '*public service officer'* is to be found in Article 358 of the Penal Code, by which '*public service officers are those who, on any basis whatsoever, provide a public service. A public service is to be understood as an activity regulated in the same manner as a public function, but which lacks powers that are typical to the exercise of a public function, and excluding the performance of ordinary tasks and merely material labour'.*

The Italian legislature clarifies the notion of 'public service' by means of two types of criteria, one positive and one negative. In order for the service to be defined as a public service, it must be regulated - as with the "public function" - by rules of public law, the difference being that there are no decision-making, authorisation and certification powers, which are proper to the public function.

Examples of public service officers are employees of supervisory authorities who do not contribute to forming the will of the authority and who do not have authorisation powers, employees of bodies that provide public services even if they are in the nature of private entities, employees of public offices, etc.

CHAPTER A.2

Offences in dealings with the Public Administration (Articles 24 and 25 of Legislative Decree 231/2001) and the offence of inducement not to make statements, or to make false statements to the judicial authorities (Article 25-decies of Legislative Decree 231/2001)

This Special Part refers to offences that may be committed in the context of dealings between the Company and the PA, as well as the offence of inducement not to make statements, or to make false statements to the judicial authorities.

A.2.1 Offences of corruption/bribery

The offence of corruption, in general, consists of a criminal agreement to exchange operational PA activities in return for the promise or delivery of money or other economic benefits by a private individual to a public official.

The mere acceptance of a promise of such a benefit is sufficient to constitute the offence. The Italian Penal Code distinguishes between 'direct' and 'indirect' corruption.

'Direct' corruption occurs when the illegitimate monetising of official duties involves an act contrary to the duties of office. The corruption is 'indirect', however, when the act in question is consistent with the duties of office.

Corruption is further divided into 'antecedent' and 'subsequent' corruption: the former arises when the benefit is agreed upon before the act is performed and with the purpose of performing it; the latter arises when the benefit is given or promised for an act already performed.

Article 321 rules out the punishability of the briber in the case of indirect subsequent corruption.

Specifically, the offence under Article 318 of the Penal Code (bribery for an official act) is committed when a public official, to perform an official act of their office, receives, for themselves or for a third party, money or other benefits as a payment to which they are not entitled, or accepts a promise of such payment.
Specifically, the offence under Article 319 of the Penal Code (bribery for an act contrary to official duties) is committed when a public official, in order to omit or delay, or for having omitted or delayed, an official act of their office or to perform or for having performed an act contrary to official duties, receives cash or another economic benefit or accepts a promise thereof, for himself or for a third party.

ACCEPTANCE OF BRIBES IN RETURN FOR THE EXERCISE OF OFFICIAL FUNCTIONS (ARTICLES 318, 320, AND 321 OF THE PENAL CODE)

The offence under Article 318 of the Penal Code is committed when a public official, in the exercise of their functions or powers, improperly receives, for themselves or for a third party, money or other benefits to which they are not entitled, or accepts a promise thereof.
By Law 190/2012, the legislature removed any reference to an official act of office already performed or to be performed.
The provision punishes both the trading of individual acts of office (previously falling under 'indirect' corruption) and corruption by subservience i.e. corruption by subservient 'selling' of one's office, where the public official is effectively placed on a private payroll, not limited to a specific act of their office. In the latter case, the public official does not merely trade a single official act of their office, but makes themselves generally available to the private party to achieve an indeterminate series of beneficial outcomes (e.g. a local government official, in exchange for company representative's promise to recruit or confer a fictitious consultancy on a family member, promises to guarantee a series of authorisations over an extended period).

ACCEPTANCE OF BRIBES IN RETURN FOR AN ACT CONTRARY TO OFFICIAL DUTIES AGGRAVATING CONDITIONS (ARTS. 319, 319-bis, 320 and 321 OF THE PENAL CODE)

The offence under Article 319 of the Penal Code is committed when a public official, in order to perform an act contrary to their official duties or to omit or delay an act of their office, receives, for themselves or for a third party, money or other benefits to which they are not entitled, or accepts a promise thereof.

For this offence to be committed in relation to an act contrary to the duties of office, consideration must be given both to acts that are unlawful (i.e. those prohibited by mandatory rules or that conflict with rules governing their validity and effectiveness) as well as acts that, although not formally unlawful, are performed by the public official in violation of the duty of impartiality or in subservience to private interests or interests alien to those of the PA.

The penalty for this offence may be increased under Article 319-bis of the Penal Code if the act contrary to the duties of office involves the awarding of public employment, salaries, pensions, or the signing of contracts involving the administration to which the public official belongs, as well as the payment or reimbursement of taxes.

Under Article 320 of the Penal Code, the provisions of Article 319 also apply to individuals entrusted with a public service. However, in such cases, the penalties are reduced by up to one-third compared to offences in which public officials are involved.

*****

Pursuant to Article 321 of the Penal Code, the penalties provided for in Articles 318 and 319 of the Penal Code also apply to anyone who gives or promises money or other benefits to a public official or public service officer.

Lastly, it should be emphasised that the offences referenced in Articles 318 and 319 of the Penal Code differ from the offence of extortion in that, in the former, there is an agreement between the bribe-giver and the corrupt party aimed at achieving a mutual advantage, whereas in extortion the private party is subject to the conduct of the public official or public service officer.

ACCEPTANCE OF BRIBES IN JUDICIAL PROCEEDINGS (Art. 319-ter of the Penal Code)

This offence is committed if a public official, such as a magistrate, court clerk or other official from the judicial authorities is bribed in order to benefit or harm a party to criminal, civil, or administrative proceedings.

UNLAWFUL INDUCEMENT BY AN OFFICIAL TO GIVE OR PROMISE AN ECONOMIC BENEFIT (ART. 319-QUATER OF THE PENAL CODE)

This offence was introduced by Law 190/2012, which separated the criminal offence of inducement, here, from the crime of extortion.

This offense is committed by public officials or public service officers who, abusing their position or powers, induce someone to unlawfully give or promise money or other benefits to themselves or to a third party. Penalties are envisaged for the public official or public service officer who induces a private individual to give or promise an economic benefit, but also for the private individual who complies with such a request.
The legislature has also extended the scope of punishability to the private individual who is at the receiving end of the inducement, but the regime of sanctions in this case is more lenient compared to the one applicable to the public servant in question.

ATTEMPTED BRIBERY/CORRUPTION (ART. 322 OF THE PENAL CODE)

This offence is committed when money or other illegitimate economic benefits are offered or promised to a public official or public service officer (to induce them to perform their duties or exercise their powers or to omit or delay implementing an official act within their competence, or to perform an act contrary to their official duties), and such an offer or promise is not accepted.

EMBEZZLEMENT, MISAPPLICATION OF FUNDS OR MOVABLE PROPERTY, EXTORTION, UNLAWFUL INDUCEMENT BY AN OFFICIAL TO GIVE OR PROMISE A BENEFIT, BRIBERY/CORRUPTION AND ATTEMPTED BRIBERY/CORRUPTION OF MEMBERS OF INTERNATIONAL COURTS OR OF EUROPEAN UNION BODIES OR OF INTERNATIONAL PARLIAMENTARY ASSEMBLIES OR OF INTERNATIONAL ORGANISATIONS, AND OF OFFICIALS OF THE EUROPEAN UNION AND OF FOREIGN STATES (ART. 322-BIS OF THE PENAL CODE)

Based on the reference to Article 322-bis contained in Article 25 of the Decree, the offences provided for in Articles 314, 314-bis, 316, 317 to 320, and 322, paragraphs III and IV, also apply when money or other economic benefits are given, offered, or promised (also after inducement) - to:

- members of the European Commission, of the European Parliament, of the Court of Justice and of the Court of Auditors of the European Union;
- officials and agents hired under contract pursuant to the Staff Regulations of Officials of the European Union, or under the rules applicable to agents of the European Union;

- persons answerable to the Member States or to any public or private body in the European Union, who perform functions corresponding to those of officials or agents of the European Union;
- members and employees of entities established under the Treaties establishing the European Communities;
- those who, within other EU Member States, perform functions or activities that correspond to those performed or carried out by public officials and public service officers;
- judges, public prosecutors, deputy public prosecutors, officials and agents of the International Criminal Court, persons answerable to States party to the Treaty establishing the International Criminal Court who perform functions corresponding to those of officials or agents of that Court, members or staff of entities established under the Treaty establishing the International Criminal Court;
- persons who perform functions or activities equivalent to those performed by public officials and public service officers in international public organisations;
- members of international parliamentary assemblies or international or supranational organisations, and judges and officials of international courts;
- persons who perform functions or activities corresponding to those performed by public officials and public service officers in non-EU Member States, when the act harms the financial interests of the Union.

The provisions of Article 319-quater(2), Article 321 and Article 322 paras. 1 and 2, also apply if the funds or other economic benefits are given, offered or promised:

- to the persons indicated in the first paragraph of this article;
- to persons who perform functions or activities corresponding to those performed by public officials and public service officers in other foreign States or international public organisations.

The persons indicated in paragraph 1 are treated as public officials, where they perform the corresponding functions, and as public service officers in other cases.

TRADING IN INFLUENCE (ART. 346-BIS OF THE PENAL CODE)

The provision in question provides for the punishment of anyone who, outside the cases of complicity in the offences under Articles 318, 319, and 319-ter, and the offences of corruption/bribery under Article 322-bis of the Penal Code, with the intent to exploit existing relationships with a public official or public service officer, or with one of the other persons referenced in Article 322-bis of the Penal Code, illegitimately obtains or promises, for themselves or others, money or other economic benefits in order to remunerate a public official or a person referenced in Article 322-bis of the Penal Code, in exchange for the performance of their functions or for carrying out a different form of unlawful mediation.

To this end, the second paragraph provides an explicit definition of a "*different form of unlawful mediation*," whereby the public servant is induced to perform an act contrary to their official duties that constitutes a criminal offence, from which an illegitimate benefit may derive.

Similarly, anyone who illegitimately gives or promises money or other benefits is also punishable.

The penalty is increased if the person who illegitimately causes money or other economic benefits to be given or promised, for themselves or others, is a public official or public service officer.
The penalties are increased, likewise, if the acts are committed in connection with the exercise of judicial functions, or to remunerate a public official or public service officer or one of the other persons referenced in Article 322-bis of the Penal Code, in relation to the performance of an act contrary to their official duties or the omission or delay of an official act of their office.
A more lenient penalty is provided if the acts in question are minor in nature.

*****

With reference to the criminal offences outlined in this section A.2.1, risk profiles for the Company arise primarily in cases where key corporate officers, members of the Board of Statutory Auditors, and/or company consultants act to bribe public officials or public service officers.
As for so-called 'passive' corruption, the Company (i.e. the natural persons who comprise it) could not commit the offence in its own right, as it lacks the necessary public law status. However, it could be complicit in a corruption/bribery committed by a public official or public

service officer if it provided the public servant in question with any form of support, material or moral (within the meaning of Article 110 of the Penal Code), in committing the offence. Note, here, that complicity in the offence of corruption also exists when one acts as an intermediary between the private individual and the public servant.

A.2.2 - Extortion

EXTORTION (ARTICLE 317 OF THE PENAL CODE)

Article 317 of the Penal Code, as amended by Law 190/2012 and Law 69/2015, punishes a public official or a public service officer who, while abusing their position or powers, compels someone to illegitimately give or promise money or other benefits to them or to a third party.

In the Civil Code formulation prior to the amendment introduced by Law 69/2015, the offence in question provided that only a public official could be an offender. With this latest amendment, the legislature extended the remit of the offence to include public service officers.

Extortion, like corruption/bribery, involves reciprocal conduct in which both the extorting party and the extorted party are involved.

However, unlike corruption/bribery, only the extorting party is subject to punishment, as the extorted party is regarded as the victim of the offence: therefore, due to the private nature of the Company's activities, its representatives are not in a position to commit the offence in their own right, as they lack the necessary public status.

Furthermore, it is theoretically possible for a company employee to hold a public function or perform a public service outside their work activities: for example, a company employee who serves as a member of a municipal city board. Such an individual must refrain, when performing their office or service, from conduct that - in violation of their official duties and/or by abusing their official functions - could illegitimately benefit the Company.

A.2.3 Fraud (Art. 24 of Legislative Decree 231/2001)

FRAUD TO THE DETRIMENT OF THE STATE OR OTHER PUBLIC BODY OR OF THE EUROPEAN UNION (ARTICLE 640(2) NO. 1 OF THE PENAL CODE)

The offence pursuant to Legislative Decree 231/01 is the aggravated case referred to in Article 640(2) no. 1 of the Penal Code, namely when the act is committed to the detriment of the State or another public entity.

This offence is committed when, in order to obtain an illegitimate gain, deceitful means are employed against an entity (including the omission of information that, if known, would have negatively or differently influenced the will of the State, another public entity or the European Union), thereby misleading that entity and causing it pecuniary loss.

The offence in question may be committed if a senior manager and/or a subordinate individual:

- resorts to any form of deception, including silence, regarding circumstances that are required to be disclosed, thereby inducing error and causing loss to the State or to another public entity, with illegitimate obtainment of a profit for themselves or others;
- uses counterfeit marks in order to make it appear that taxes and contributions have been paid;
- communicates false data or prepares false documentation in order to obtain public funding.

AGGRAVATED FRAUD TO OBTAIN PUBLIC FUNDS (ART. 640-BIS OF THE PENAL CODE)

This offence is committed when the acts referred to in the aforementioned section of Article 640 of the Penal Code are carried out in order to obtain contributions, funding, or other disbursements from the State or other public entities.

For example, improperly obtaining public funding aimed at supporting business activities in specific sectors by producing false documentation attesting to the presence of the requirements for obtaining the funding.

COMPUTER FRAUD (ART. 640-TER OF THE PENAL CODE)

The offence of computer fraud is committed when, in order to obtain an illegitimate gain for oneself or others, to the detriment of other persons, the functioning of a computer system is altered in any way, or when there is illegitimate and unauthorised interference with data, information, or programs contained in a computer system.

This offence is relevant for the purposes of the Decree only if committed to the detriment of the State or another public entity.

For example, the offence is committed by altering information on the accounting status of a contractual relationship with a public entity, or by falsifying tax and/or social security data contained in a PA database.

A.2.4 Offences of embezzlement and misappropriation of public funds

EMBEZZLEMENT OF PUBLIC FUNDS (ART. 316-BIS OF THE PENAL CODE)

This offence is committed by anyone who, having obtained contributions, grants, funding, subsidised loans or other similar disbursements, however named, from the State, another public entity or from the European Union, which are designated towards one or more public interest purposes, fails to allocate them to such activities.

For the offence to be committed, it is enough that even only a portion of the funds received is used for purposes other than those intended, regardless of whether the planned activity was carried out or not. The perpetrator's actual purposes are also irrelevant, because the subjective element of the offence (*mens rea*) consists of the intent to divert resources that were intended for a predetermined purpose.

A typical example is the receipt of public funds aimed at facilitating the recruitment of persons from special categories, and this purpose is later disregarded.

MISAPPLICATION OF FUNDS OR MOVABLE PROPERTY (ART. 314-BIS OF THE PENAL CODE)

The offence of '*misapplication of funds or movable property'* is an offence against the Public Administration that is specific to a certain category of offender, namely public officials (Article 357 of the Penal Code) and public service officers (Article 358 of the Penal Code).

The provision, which begins with a specific reservation clause making the offence subsidiary to the main offence category of embezzlement (Article 314 of the Penal Code), punishes a public official who allocates funds or other movable property belonging to others - in their possession or control by reason of their office or service - to a use other than that prescribed by specific legal provisions or acts having the force of law, which leave no room for discretion.

This new offense also requires proof of intent: the individual must have acted deliberately to gain an illegitimate financial advantage (for themselves or someone else) or to cause illegitimate harm to another.

This type of offence lies midway between the old offence of embezzlement by diversion of public funds (*peculato per distrazione*) and the repealed offence of abuse of office. This new offence was introduced as a predicate offence under Article 25 of the Decree only in cases *where the act causes detriment to the financial interests of the European Union.*

UNLAWFUL RECEIPT OF PUBLIC FUNDS (ART. 316-TER OF THE PENAL CODE)

The offence is committed when a person - by using or presenting false declarations or documents or those attesting to untrue facts, or by omitting required information - illegitimately obtains grants, subsidies, contributions, loans, subsidised loans or similar disbursements, however named, which are granted or disbursed by the State or other public bodies or by the European Union.

In this case, unlike the previous offence, the use made of the disbursements is irrelevant, as the offence is committed at the moment the funds are obtained.

Finally, it should be noted that this offence is residual in relation to the offence under Article 640-bis of the Penal Code (aggravated fraud in order to obtain public funds), in that it only applies in cases where the conduct does not meet the offence criteria provided in the said Article 640-bis.

FRAUD IN PUBLIC PROCUREMENT (ART. 356 OF THE PENAL CODE)

The perpetrator in this offence category commits deception while engaged in performing supply contracts or fulfilling contractual obligations arising from a supply contract entered into with the State or with another public entity, or with a company providing public services and/or essential public services.

*****

In relation to the offences under Articles 316-bis, 316-ter and 640-bis of the Penal Code, note that contributions and subsidies are non-repayable financial allocations that may be periodic or one-off, fixed in amount or determined based on variable parameters, and may be tied to specific conditions or may be purely discretionary; loans are private legal transactions involving an obligation to allocate sums of money or to repay them, or additional and different responsibilities. Subsidised loans are disbursements of money with an obligation to repay the same amount but with interest rates lower than those available on the market.

INTERFERENCE IN PUBLIC OR PRIVATE TENDERING/BIDDING PROCEDURES (ART. 353 OF THE PENAL CODE)

This offence is committed when any person, with violence, threats, gifts, promises, collusion or other fraudulent means, prevents or disrupts a public or private bidding procedure on behalf of public administrations, or anyone who deters bidders from participating.

INTERFERENCE WITH THE FREEDOM TO CHOOSE A CONTRACTOR (ART. 353-BIS OF THE PENAL CODE)

Unless the act constitutes a more serious offence, this offence is committed when a person, through violence, threats, gifts, promises, collusion, or other fraudulent means, disrupts an administrative procedure aimed at determining the content of a tender or equivalent procedure, with the aim of influencing the PA's choice of contractor/contracting party.

*****

INDUCEMENT NOT TO MAKE STATEMENTS, OR TO MAKE FALSE STATEMENTS TO THE JUDICIAL AUTHORITIES (ART. 377-BIS OF THE PENAL CODE)

The Law 116/2009 introduced Article 25-decies into Legislative Decree 231/2001, establishing the relevance for the Decree's purposes of the offence of "*Inducement not to make statements, or to make false statements to the judicial authorities*" pursuant to and punishable under Article 377-bis of the Penal Code.

Under this article, unless the act constitutes a more serious offence, any person shall be punished in accordance with law if he/she, with violence or threats or the offer or promise of money or other benefits, induces a person summoned to make statements before the judicial authorities which may be used in criminal proceedings, to withhold statements or to make false statements, when such person has the right to remain silent.

CHAPTER A.3

A.3.1 Sensitive Processes associated with dealings with the Public Administration and with the offence of inducement not to make statements or to make false statements to the judicial authorities

The following are the main Sensitive Processes of relevance to the offences under consideration, which the Company has identified within its organisation:

- management of dealings with public bodies with a view to obtaining authorisations, concessions and permits for the performance of various company activities;
- management of periodic audits/inspections carried out by designated personnel from various PA authorities and administrations;
- general management of dealings with the PA (e.g. management of dealings with various authorities (the Italian Customs Agency, Tax (Financial) Police; Local Health Authorities (ASL), Italian Tax Authority, Municipalities, Provinces, Regions, Labor Inspectorate, National Institute for Insurance against Occupational Accidents (INAIL), Carabinieri etc.) for communication exchanges, management of dealings with the Italian tax authorities for tax and fiscal compliance obligations, management of dealings with public officials and public service officers in general, management of dealings with social security and welfare institutions for pay and social security-related compliance obligations involving employees and non-company collaborators, management of dealings with public authorities in charge of workplace health and safety;
- granting of delegated powers or powers of attorney for purposes of mediating with the PA;
- participation in procedures for obtaining disbursements, grants or subsidised loans from Italian or EU public bodies;
- management of dealings in which the PA is the client's counterparty;
- management of legal matters and of disputes in or out-of-court;
- management of monetary and financial flows (e.g. management of accounting and payments);
- management and use of technological infrastructures and information and electronic telecommunications systems (e.g. transmission of data on electronic media to public administrations);
- management of voluntary donations (e.g. management of freebies, gifts, sponsorships and donations).

CHAPTER A4

A.4.1 The system in general

The aim of this Special Part is to ensure that all Recipients adopt rules of conduct in compliance with its provisions, in order to prevent the occurrence of the offences considered therein.

All Sensitive Processes must be implemented in conformity with applicable laws, with the values and policies of the Company, and with the rules set out in this Model.

In general, the Company's organisational system must adhere to the fundamental requirements of formalisation and clarity, communication, and separation of roles, particularly with regard to the assignment of responsibilities, representation, hierarchical lines and operational activities.
The Company must be equipped with organisational tools (organisation charts, internal communications, procedures, etc.) based on the following general principles:

a) that these organisational are capable of being known and disseminated inside the Company;
b) the clear and formal delineation of roles: providing a complete description of the tasks of each function and the related powers.

Internal procedures must be characterised by the following features:

a) optimum separation, within each process, between the individual who initiates the process (decision source), the individual who executes and concludes it, and the individual who controls it;
b) traceability in terms of written records of each material step in the process;
c) adequate level of formalisation;
d) care to ensure that reward systems for individuals with spending powers or decision-making powers, with effects outside the Company, are not based on substantially unachievable performance targets (i.e. when operating lawfully).

A.4.2 System of delegated powers and powers of attorney

The system of delegated powers and powers of attorney at GIMA S.p.A. is (and must be) structured so as to ensure the following: the allocation of responsibilities, the segregation of activities between the different persons who authorise, implement, record and control operations conducted within the Company's "at-risk" activities (i.e. those vulnerable to the commission of offences under the Decree) and, lastly, compliance with a series of control principles adopted by the Company, all in conformity with the corporate governance system and the organisational system implemented by GIMA.

In any case, no individual shall independently manage an entire process, in adherence to the principle of separation of functions implemented by the Company.

The Management Body, Managers and function heads involved in at-risk activities and in the related instrumental processes, as well as collaborators involved in the management of at-risk activities, are considered persons responsible (*responsabili*) and direct points of reference for each at-risk operation carried out directly or within the scope of their respective functions.

With regard to delegated powers and powers of attorney, persons interacting with the Public Administration must be provided with a formal delegated power to this effect that clearly indicates the limits and purpose thereof.

The system of delegated powers and powers of attorney must be characterised by elements of "certainty" in order to prevent the commission of offences, and must facilitate the efficient management of company activities. An organisational ‘delegated power’ is any internal act by which functions and responsibilities are assigned, as reflected in the system of organisational communications. An organisational ‘power of attorney’ is a unilateral legal act by which the Company grants an individual the authority to act on its behalf.

The essential requirements of the system of delegated powers and powers of attorney are as follows:

a) all individuals who interact with the Public Administration on behalf of the Company must be equipped with a formal delegated power to that effect and, where necessary, with a power of attorney;
b) each power of attorney granting the power to represent the Company before third parties must correspond to an internal delegated power that describes the associated management power;
c) the grant of delegated powers must associate each managerial power with the related responsibility and with a sufficiently senior role in the organisation chart;
d) each grant of delegated powers must specifically and unequivocally define:

1. the powers of the delegatee, specifying their limits;
2. the person (body or individual) to which/whom the delegatee reports hierarchically.

e) the delegatee must be granted spending powers adequate to discharge the functions assigned;

f) the power of attorney must explicitly provide for cases of termination of the conferred powers (revocation, transfer thereof to incompatible job roles, dismissal, etc.);
g) the system of delegated powers and powers of attorney must be promptly updated.

No individual shall be granted unlimited powers; powers of authorisation and signature are assigned based on the delegatee's role in the Company, taking into account their hierarchical level, in compliance with company procedures and with the power and authorisation levels provided therein.

The system of delegated powers and powers of attorney must ensure that each individual's position and corresponding responsibilities are in alignment with the powers granted.

If an individual should cease to hold a specific function or position, his/her delegated powers and powers of attorney must be revoked or amended without delay.

The Supervisory Body periodically verifies, with the support of other competent functions, the current system of delegated powers and powers of attorney and their consistency with the entire system of organisational communications, recommending any necessary changes where the management authority and/or job status fails to reflect the nature of the delegated powers granted, or if other anomalies are identified.

The system of delegated powers and powers of attorney represents a set of control standards ('protocol') applicable to all Sensitive Processes.

A.4.3 General Principles of Conduct

The following general principles apply to Recipients of the Model, both directly and through specific contractual clauses.

First and foremost, it is prohibited to engage in, collaborate in or cause or produce conduct or behaviours that, considered individually or together, directly or indirectly instantiate the offences outlined above; violations of the principles and procedures set out in this Special Part are also prohibited.

In the context of the aforementioned conduct, it is forbidden, in particular:

a) to make monetary payments to Italian or foreign public officials;

b) to grant benefits of any kind whatsoever to the representatives of Italian or foreign Public Administrations, if they produce the same consequences as outlined in the previous paragraph;

c) in any context, to provide untrue information to the PA or to induce third parties to do so;

d) to provide services or award payments to consultants, suppliers and partners that cannot be suitably justified by the contractual relationship with them, depending on the type of assignment to be carried out and on local business practices;

e) to submit untrue/false statements to Italian or EU public bodies in order to obtain public disbursements, or contributions or subsidised loans;

f) to allocate monies received from Italian or EU public bodies, as disbursements or contributions or loans, to purposes other than those for which they were intended.

CHAPTER A.5

Specific procedural principles

A.5.1 Specific procedural principles of general application

In order to implement the rules and prohibitions listed in the previous Chapter, in addition to the General Rules and Principles already contained in the General Part of this Model, the principles set out below must be adhered to.

The rules described below must be adhered to in the conduct of the Company's activities, both in Italy and abroad.

A.5.2. Specific procedural principles related to Sensitive Processes

In relation to the Sensitive Processes identified Chapter A.3 above, the Company – also by adopting special procedures – ensures compliance with the following specific principles:

1) Management of dealings with the Public Administration (e.g. when applying for and obtaining authorisations, licences, permits and concessions to perform company activities, management of dealings with public when seeking contributions, disbursements, loans and/or tax credits; management of inspections).

1. Recipients of the Model who substantively interact with the PA on the Company's behalf shall, where necessary, be granted formal authority to do so by the Company (with specially delegated powers for employees and governing bodies and, for the other persons indicated, with powers indicated in the relevant mandate or consultancy or partnership agreement). Where necessary, the aforementioned persons may be issued with a special written power of attorney that observes all the criteria set out in the General Part of this Model;
2. any Recipients of the Model who substantively interact with the PA on behalf of the Company must continuously inform the Managing Director (and periodically inform the Supervisory Body) about the outcomes of meetings with the PA, particularly when these are of significant importance (e.g. where they deal with inspections rather than purely executive/technical meetings);
3. the Supervisory Body shall be promptly notified in writing of any critical issues or conflicts of interest that arise in the context of dealings with the PA.
4. at least two expressly delegated individuals must be present at judicial, tax, and administrative inspections, and also at any face-to-face interactions with the PA;
5. official minutes of the entire inspection process or of any face-to-face interactions with the PA must be drawn up and retained. If the final minutes should highlight critical issues, the head of the function concerned must send a copy thereof to the Supervisory Body;
6. all correspondence with the PA must be traceable (registered mail, certified email) and duly archived;
7. individuals who interact with the PA on the Company's behalf must receive adequate training on the standards and principles of conduct which they are required to uphold in the context of such dealings.

2) Application for and management of public funding

a) The roles and responsibilities attributable to internal functions involved in requesting and managing public disbursements (including in the form of tax incentives) must be specifically identified, in compliance with the principle of role segregation and dual control. These individuals are responsible, among other things, for:

1. making a preliminary assessment – potentially carried out with the advice of consultants – of the Company's eligibility for the disbursement;

2. checking whether the qualifying criteria justifying the receipt of the disbursement continue to be met over time;

3. checking whether, in cases where the disbursement has been made for specific purposes, it has in fact been deployed for such purposes;

4. producing and submitting special updates/reports to the management body and Supervisory Body on the management in general of public disbursements;

b) the Company ensures that the content of all information communicated to the PA is true and accurate and that dealings with public officials aimed at the fulfilment of all pre- and post-funding obligations for public funding and any type of public disbursement in general (including obligations of reporting to the disbursing entity), are conducted in compliance with the principles of transparency and correctness;

c) the Company has a special authorisation process for senior managers in connection with its participation in public tenders or for the submission of requests to obtain loans, public disbursements and public funding of any kind (from the Italian PA or from EU institutions and bodies);

d) the Supervisory Body must be informed of any critical issues identified in relation to public disbursements.

3) Management of dealings with the judicial authorities (management of proceedings in which the entity is involved as a plaintiff or defendant or as an interested third party) and participation of key corporate officers in criminal proceedings

a) All of the terms and conditions of all dealings between the Company and consultants involving the management of litigation/disputes shall be drawn up in writing, and those dealings shall comply with the provisions below, in relation to the Sensitive Process "*Selection of Suppliers and Consultants and management of related dealings*";

b) consultants who assist the Company with litigation/disputes are required, when initially hired and periodically thereafter, to provide documentation proving that they satisfy the necessary standards of professionalism and integrity, and are obliged to promptly inform the Company if they no longer satisfy those standards (for example, if have been subject to disciplinary sanctions by their professional association);

c) the Supervisory Body must be informed in writing of the status of proceedings involving the Company, and should be periodically updated on any significant events, such as important hearings attended by Company representatives.

A.5.3. Specific procedural principles related to activities instrumental to the commission of offences against the Public Administration

In order oversee Sensitive Processes and limit the risk of commission of offences against the PA, the Company – also by adopting specific procedures – adheres to the following specific principles in the context of 'instrumental activities':

a) Selection and recruitment of personnel

1. The roles and responsibilities of internal functions involved in the personnel selection and recruitment process should be specifically identified, in compliance with the principle of role segregation and dual control;
2. the personnel selection and recruitment process should follow transparent criteria based on the following parameters:

i. the personnel selection and recruitment process should be structured across multiple phases, involving multiple functions/individuals;
ii. application of objective criteria – based on merit and professionalism – in choosing the most suitable candidate for recruitment and determining their work category and remunerations and contract terms;
iii. verification in advance of the absence of impediments to recruitment, and also of professionalism adequate to the candidate position or job duties in question;
iv. exclusion of any interference by third parties in the recruitment process of employees;
v. retention of documentation related to the selection process, also in order to facilitate its consultation by the Supervisory Body in the context of its oversight function;

3. any internal career advancements and awards (including the possible inclusion of a variable component in the remuneration, linked to the achievement of specific targets) must be granted according to objective criteria, based on merit and professionalism. In general, the Company does not tolerate unlawful conduct by employees aimed at achieving targets that result in rewards; in particular:

i. the grant of incentive payments such as bonuses should be based on the achievement of predetermined targets;
ii. career advancements are evaluated based on professional qualifications and on the outcome of performance review meetings conducted with the function manager;

the Company guarantees that each new recruit:

i. receives an updated copy of the Company's Model when the employment relationship is created;
ii. signs a declaration of receipt and commitment to comply with the Model;
iii. receives, as part of the new recruit's initial training activities, foundational training on the legislation, principles and standards referenced in the Decree.

b) management of gifts, donations and sponsorships

a) It is forbidden to offer gifts, free services, or other forms of donation other than in accordance with company practice. In particular, no form of donation, gift, freebie or free service shall be offered, directly or indirectly, to PA representatives or to their family members if they could be seen as linked to the Company's activities or aimed at influencing the recipient's independent judgment, or inducing them to secure any illegitimate benefit for the Company. In general such gifts, free services or donations shall not exceed EUR 150.00 in value. Even if the relevant individuals come from countries where offering donations or gifts is a widespread courtesy practice, gifts should be appropriate, comply with legal provisions and should not be interpreted as a request for favours in return;

b) the Company has specific approval processes for permitted gifts or donations, as well as a list of acceptable gifts/donations;

c) any derogation from the safeguards in place for gifts or donations needs senior management involved, and must be notified to the Supervisory Body;

d) a process is in place to evaluate requests (or independent initiatives) for corporate gifts/sponsorships, aimed at ascertaining the credentials of the requesting entity (or recipient);

e) the Company ensures that the Supervisory Body receives periodic (annual) reports on gifts, sponsorships and donations made during the reporting period.

c) Management of Expense Reimbursements

a) The Company establishes specific limits and procedures for reimbursing expenses incurred by company representatives and employees in the course of business activities;

b) all expense claims are recorded;

c) all travel and entertainment expenses incurred by the Company's staff and consultants must be supported by appropriate documentation and justified by their direct relevance to work activities;

d) expenses exceeding a certain threshold may only be reimbursed if pre-approved;

e) incurred expenses are reimbursed by reference to a traceable documentation trail.

d) Management of financial flows

a) The Company guarantees that individuals authorised to carry out any financial transaction are identified - in advance and retrospectively - by means of special powers of attorney that specify their spending powers (including any approval thresholds based on expenditure amounts);

b) the Company's financial management tasks include formal and substantive checks on incoming and outgoing financial flows. These checks consider as a basis the counterparty's registered office and the destination or origin of the incoming or outgoing funds (e.g. so-called tax havens, countries on international blacklists, etc.);

c) the Company checks in advance that the payment recipient's account is not registered under a different name or located in a country other than where the recipient is based;

d) any increases in the price list already agreed with suppliers, and any different economic conditions such as discount percentages applicable to orders, must be communicated/agreed in writing (even in cases where no formal contract has been signed with the supplier);

e) it is expressly prohibited to make payments using non-traceable methods,, except for small amounts (processed through the "petty cash" fund), which must nevertheless be duly authorised and documented;

f) before proceeding with payment, checks are conducted to ascertain whether services agreed with suppliers and consultants have actually been provided, and to ascertain the appropriateness of the price agreed;

g) the persons responsible for checking and overseeing activities linked to the fulfilment of the above sensitive processes (e.g. invoice payments, allocation of funds obtained from the State or other bodies) must immediately report any irregularities or anomalies to the Supervisory Body.

e) Selection of suppliers and consultants, negotiation of agreements and management of dealings

a) All of the terms and conditions of all dealings between the company, suppliers and consultants shall be drawn up in writing, and those dealings shall comply with the provisions outlined in the paragraphs below (such relationships shall be governed by written agreements, at the very least the economic terms and conditions of the supply/consultancy relationship);

b) Suppliers and consultants shall be selected by reference to transparent processes - based on objective criteria that value merit and professionalism - and according to standardised procedures, which may involve competitive processes; alternatively, pre-approved parties may be used who have been included in a special vendors list (this document lists suppliers and consultants who have proven to be trustworthy and have had a long-standing relationship with the Company, as outlined below);

c) the Company ascertains the professionalism and integrity of suppliers and consultants at the initial recruitment stage and periodically thereafter, requiring them to inform the Company, in good time, of any loss of such qualifications (e.g. in the event of a conviction for an offence under the Decree);

d) the Company formalises a so-called vendor list of loyal suppliers whom it uses periodically or on an ongoing basis, which indicates the supplier's name and annual turnover, and any key formalities adopted within the commercial relationship in question (e.g. whether a fixed rate is used or prices are negotiated case by case, whether purchase orders are used or a supply contract has been signed);

e) contracts with suppliers and consultants must include standard "*Model 231 Clauses"* ;

f) where relationships with suppliers/consultants are already in place or cannot be regulated by a formal written contract, the Company sends suppliers/consultants a "231 Notice", requesting their signature, which includes the Model 231 Clauses referred to in the previous paragraph.

CHAPTER A.6

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the limits of their respective duties and responsibilities, properly observe the rules and principles enshrined in this Special Part and in the company procedures to which that Part explicitly or implicitly refers.

In particular, it is the responsibility of the SB:

- to monitor the effectiveness of the procedural principles provided therein, or of the principles contained in company policies adopted for the prevention of offences outlined in this Special Part;
- to propose any necessary changes to Sensitive Processes attributable to potential changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties, or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The SB shall be promptly informed of any infringements of the specific procedural principles contained in this Special Part, or of infringements of company procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART - B -

Corporate offences (including bribery/corruption among private individuals)

CHAPTER B.1

Corporate offenses (Art. 25-ter of Legislative Decree 231/2001)

This Special Part refers to corporate offences and offences of bribery/corruption among private individuals, as outlined in Art. 25-ter of the Decree. Below is a brief description of the offences covered in this Special Part, as indicated in Art. 25-ter of the Decree ("corporate offences", below).

B.1.1 Offences of falsification

FALSE CORPORATE REPORTING (ART. 2621 OF THE ITALIAN CIVIL CODE)

The offence under Art. 2621 of the Italian Civil Code is committed when, knowingly, '*with the aim of obtaining an illegitimate gain for oneself or others, relevant material facts that do not correspond with the truth are presented in financial statements, reports or in other corporate communications required by law, addressed to shareholders or the public, or when information relevant to the profit-and-loss, capital and financial position of the company or the group to which it belongs is omitted, despite its disclosure being required by law, in a manner likely to mislead recipients about that position'*.

Those who may be liable for such offences include directors, general managers, managers charged with preparing the company's corporate accounting documents, auditors, and liquidators.

Note that:

- pursuant to Article 2621-bis of the Civil Code, the penalty may be reduced if the facts referenced in the aforementioned provision are of minor significance, or concern companies that do not exceed the limits indicated in Art. 1(2) of Royal Decree no. 267 of 16 March 1942;
- pursuant to Article 2621-ter of the Civil Code, the conduct is not punishable if the act is of minimal significance.

FALSE OR OMITTED DECLARATIONS FOR THE ISSUANCE OF PRELIMINARY CERTIFICATES (ART. 54 OF LEGISLATIVE DECREE 19/2023)

This offence could be committed in the context of a cross-border merger carried out by the Company. Such an offence could arise if documents to be submitted to the Notary Public for the issuance of a preliminary merger certificate are altered or falsified, or if false declarations are made to the Notary Public or if the latter is not provided with relevant information for the issuance of the aforementioned certificate. The aim is to make it appear that the conditions required by law for the issuance of the certificate have been met.

Specifically, Article 29 of Legislative Decree 19/2023 provides that, upon request by the Italian company participating in the cross-border merger, the Notary Public issues the preliminary

certificate attesting to the regular fulfilment, in accordance with law, of all relevant acts and compliance formalities preliminary to the formalisation of the merger.

B.1.2 Protection of share capital

ILLEGAL REPAYMENT OF CONTRIBUTIONS (ARTICLE 2626 OF THE ITALIAN CIVIL CODE)

This offence, like the one provided for in the subsequent Article 2627 of the Italian Civil Code, seeks to protect of the integrity of share capital and is committed when the directors, without legitimate justification to reduce the share capital, proceed to return (also in an equivalent form) contributions made by shareholders, or release shareholders from their obligation to make such contributions. The offence in question is relevant only when the directors's actions affect the share capital, and not the funds or reserves. For the latter, the relevant offence is the one provided for in Art. 2627 of the Civil Code.

The return of contributions may be overt (when directors return assets to shareholders without receiving any payment or issue declarations aimed at releasing shareholders from their payment obligations) or, more likely, underhand (when directors use deceptive schemes such as distributing fictitious profits using sums withdrawn from the share capital rather than the reserves, or offsetting the company's receivables against non-existent receivables claimed by one or more shareholders).

Only directors are liable for this offence. The law, in other words, does not seek to punish shareholders who benefit from the return or release of the share capital, thus 'essential' complicity is not present. However, there remains the possibility of 'contingent' complicity, by which shareholders who have instigated or determined the directors' unlawful conduct may also be held liable for the offence, in accordance with the general rules of complicity under Article 110 of the Italian Penal Code.

UNLAWFUL DISTRIBUTION OF PROFITS AND RESERVES (ART. 2627 OF THE ITALIAN CIVIL CODE)

This offence consists of the distribution of profits (or advances on profits) not actually achieved or allocated by law to reserves, or the distribution of reserves (including those not created from profits) that cannot be distributed by law.

Directors are liable for this offence. The law, in other words, does not seek also to punish shareholders who benefit from the distribution of profits or reserves, thus 'essential' complicity is not present. However, there remains the possibility of 'contingent' complicity, by which shareholders who have instigated or determined the directors' unlawful conduct may also be held liable for the offence, in accordance with the general rules of complicity under Article 110 of the Italian Penal Code.

UNLAWFUL DEALING IN THE STOCKS OR SHARES OF THE COMPANY OR OF ITS PARENT COMPANY (ART. 2628 OF THE ITALIAN CIVIL CODE)

This offence is committed by the purchase or the subscription, outside permissible legal limits, of shares or units issued by the company (or the parent company) that cause harm to the integrity of the share capital or reserves that are non-distributable by law.

The provision is aimed at protecting the integrity of the share capital and must be read in conjunction with the analysis under Article 2357 of the Civil Code, which provides that limited companies taking the form of the S.p.A. (*società per azioni*) cannot not purchase their own shares, including through a trust company or an intermediary, save within the limits of distributable profits or available reserves as indicated in the most recently approved financial statements. The provision requires that the shares must be fully paid up.

The offence may be committed not only in the event of simple purchase, but also in cases where the title to the shares is transferred, for example, through swap contracts or contango contracts, or where shares are transferred without valuable consideration, such as donation.

Directors are liable for this offence. The directors of a parent company may incur liability for complicity with the directors of a subsidiary where the latter conduct illicit transactions involving the parent company's shares at the instigation of the former.

TRANSACTIONS TO THE DETRIMENT OF CREDITORS (ART. 2629 OF THE ITALIAN CIVIL CODE)

This offence is committed when, in breach of legal provisions protecting creditors, reductions of share capital, mergers with another company, or demergers are carried out, which cause harm to creditors.

Note that:

- the payment of compensation for loss to creditors before legal proceedings will have the effect of extinguishing the offence;
- the offence is punishable upon complaint by the injured party;
- directors are liable for this offence.

FICTITIOUS CAPITAL FORMATION (ART. 2632 OF THE ITALIAN CIVIL CODE)

This offence is committed with the following conduct:

- the share capital or part thereof is fictitiously formed or increased, by allocating shares or units in a total amount exceeding the share capital;
- reciprocal subscription of shares or units; significant overvaluation of contributions in kind, of credits, or of the company's assets in a company restructuring.

Directors and contributing shareholders can be held liable for this offence.

B.1.3 Safeguarding the proper operation of the Company

OBSTRUCTION OF THE GOVERNING AND AUDIT BODIES IN THE COURSE OF THEIR DUTIES (ART. 2625 OF THE CIVIL CODE)

This criminal offense is committed when, by concealing documents or by other deceptive schemes, the audit/control activities legally attributed to shareholders or to the other governing bodies are obstructed.

The offence can only be committed by directors.

B.1.4 Criminal protection against fraud

MANIPULATION OF STOCK MARKET TRANSACTIONS (ARTICLE 2637 OF THE CIVIL CODE)

This offence punishes persons who disseminate false information or engage in sham transactions or other deceptive schemes that could lead to significant changes in the price of unlisted financial instruments, or those for which no request for admission to trading on a regulated market has been made, or which could significantly affect the public's trust in the financial stability of banks or banking groups.

Consider, for example, a case where the Company disseminates studies on unlisted companies containing exaggerated and/or false data forecasts and recommendations.

This is also a 'common' offence, which can be committed by any person engaging in the criminal conduct.

CHAPTER B.2

B.2.1 Bribery/corruption among private individuals (Art. 25-ter(I), Letter s-bis, of Legislative Decree 231/2001)

Law 190/2012, containing '*Measures for the prevention and suppression of corruption and illegality in the public administration'*, introduced the offence of '*bribery/corruption among private individuals'* into our legal system, by amening Art. 2635 of the Civil Code, which originally punished '*breach of trust following the giving or promise of benefits'*.

The Article in question has since been further amended and now reads as follows:

'1. Unless the act constitutes a more serious offence, directors, general managers, managers in charge of drafting corporate accounting documents, auditors and liquidators of companies or private entities, who, including through an intermediary, for themselves or for others, solicit or receive money or other illegitimate economic benefits or accept promises thereof, in exchange for performing or omitting to perform an act in breach of the obligations of their office or of their fiduciary duties, are punishable by a term of imprisonment from one to three years. The same penalty shall apply if the act is committed by anyone within the organisational structure of the company or private entity who exercises managerial functions other than those of the persons referenced in the preceding sentence.

2. The penalty of imprisonment up to one year and six months shall apply if the act/conduct is committed by anyone subject to the direction or management of one of the persons referred to in the first paragraph.

3. Any person who, including through an intermediary, offers, promises or gives money or other illegitimate economic benefits to the persons referred to in the first and second paragraphs shall be punished by the penalties provided therein.

4. The penalties provided in the previous subsections shall be doubled in the case of a company with securities listed on regulated markets in Italy or other European Union states or widely distributed to the public within the meaning of Art. 116 of the Consolidated Law on Financial Intermediation, referred to in Legislative Decree no. 58 of 24 February 1998, as amended.

5. Without prejudice to the provisions of Art. 2641, the value-based confiscation measure shall not be less than the value of the economic benefits given, promised, or offered'.

Legislative Decree 38/2017 introduced a new offence into the legal system, namely '*incitement to bribery/corruption among private individuals'* provided for and punishable under Article 2635-bis of the Civil Code. The Article in question – also included among the predicate offences – has since been further amended and now reads as follows:

'1. Anyone who offers or promises money or other illegitimate economic benefits to directors, general managers, managers responsible for preparing corporate accounting documents, to auditors and liquidators of private companies or entities, and to anyone performing managerial functions therein, in order to induce them to perform or to omit an act in violation of the obligations of their office or of their obligations of trust, shall be subject - if the offer or promise is not accepted - to the penalty provided in the first paragraph of Art. 2635, reduced by one-third.

2. The penalty referred to in the first paragraph shall apply to directors, general managers, officers responsible for preparing corporate accounting documents, to auditors and liquidators of private companies or entities, and to anyone performing managerial functions therein, who request or solicit, for themselves or others, including through an intermediary, a promise or a gift of money or other benefits, in order to perform or to omit an act in violation of the

obligations of their office or of their obligations of trust, if the request or solicitation is not accepted'.

The 'active' nature of the offence of bribery/corruption among private individuals is relevant for the purposes of the administrative liability of entities under the Decree, based on the reference contained in Art. 25-ter, letter s-bis, of the Decree to the third paragraph of Art. 2635 ('*Anyone who, including through an intermediary, offers, promises, or gives* [...]') and to the first paragraph of Art. 2635-bis of the Civil Code ('*Anyone who offers or promises* [...]').

CHAPTER B.3

B.3.1 Sensitive Processes in the context of corporate offences

The following are the main Sensitive Processes of relevance to the offences under consideration, which the Company has identified within its organisation:

1) maintaining accounts, preparing the financial statements, preparing communications relevant to the company's profit-and-loss, capital and financial position;
2) external communications: management of outbound corporate data and reports (communications with shareholders, the general public and with the various authorities);
3) influencing the Shareholders' Meeting;
4) capital transactions;
5) corporate restructuring or reorganisation processes.

B.3.2 Sensitive Processes and instrumental activities in the context of offences of bribery/corruption among private individuals

The following are the main Sensitive Processes relevant to the offences of bribery/corruption among private individuals that the Company has identified within its organisation:

1) managing dealings with certification bodies;
2) managing disputes and entering into settlement agreements;
3) managing dealings with lending institutions and insurance companies.

The following activities, on the other hand, are considered to be activities instrumental to the commission of offences of bribery/corruption among private individuals:

1. selection and recruitment of personnel;
2. management of gifts, donations and sponsorships;
3. management of expense reimbursements;
4. management of financial flows;
5. selection of suppliers and consultants, negotiation of related agreements and management of related relationships.

CHAPTER B.4

General Principles of Conduct

This Special Part expressly forbids employees and governing bodies of the Company from engaging in, collaborating in, or causing conduct or behaviours that, individually or together, directly or indirectly, trigger the predicate offences outlined above (Art. 25-ter of Legislative Decree 231/2001) or that, although not in themselves materialising an offence, may be preparatory to such offences (e.g. lack of control). Recipients must also avoid any infringement of the principles and company procedures that are potentially relevant to this Special Part.

In general, within the context of corporate offences:

a) all corporate communications shall be drafted in a way that ensures that the data and information provided by each function are clearly and comprehensively indicated, as well as the accounting criteria for data processing, and the time frames for their delivery to the responsible functions;

b) the recording of financial data and their formulation to facilitate in preparing the draft financial statements must conform to the principles of veracity, accuracy, precision, and completeness of data and information contained in the financial statements or other accounting documents, and in related documents;

c) all capital transactions, the incorporation of companies, the acquisition and disposal of shareholdings, mergers and demergers, must be carried out in compliance with applicable laws.

In relation to the offences of bribery/corruption among private individuals, all Recipients of this Model are, in general, forbidden to engage in conduct that may, directly or indirectly, trigger such offences. More specifically, all Recipients of this Model are prohibited from:

a) promising, granting or authorising any undue remuneration or other benefit to bribable individuals (directors, general managers, managers responsible for preparing accounting documents, auditors, liquidators or individuals exercising other managerial functions), employees, and any collaborators of companies or consortia;
b) using intermediaries, such as suppliers, consultants, or other third parties, to channel payments that are intended to be received by bribable individuals, their friends or family members, and also by companies, non-profit associations, employees, or business partners attributable to them.

All Recipients of this Model – and in particular those who engage in commercial dealings with suppliers, consultants, and any other contractual counterparties – are required to act transparently, ethically, with integrity and in good faith, in full compliance with legislative and regulatory provisions applicable in Italy and with company rules and standards, also in order to safeguard free and fair competition among businesses.

Furthermore, all Recipients of this Model undertake to report to the Supervisory Body any conduct that could, directly or indirectly, trigger the offence of bribery/corruption among private individuals.

The Company, in turn, in order to avert bribery/corruption:

a) ensures that spending powers are appropriate to the relevant roles and responsibilities within the company's organisational structure, and also to ordinary operational needs;

b) adopts remuneration policies for management that are in line with strategic objectives, profitability and the long-term equilibrium of the company, avoiding policies that are based exclusively or predominantly on difficult-to-achieve results and/or those that may encourage Recipients to engage in illicit behaviour;

c) in the context of the management of finances and accounting, adopts company procedures that are designed to ensure that all incoming and outgoing financial flows are correctly and regularly tracked and that no secret accounts or unrecorded entries are created;

d) ensures that the selection and recruitment of employees complies with company procedures that include multiple progressive steps (from the creation of the position to the authorisation of

the contract) as well as, in general, assessment criteria based on the professionalism and merit of candidates.

CHAPTER B.5

Specific procedural principles related to Sensitive Processes identified in connection with corporate offences

In order to implement the rules listed in the previous Chapter, in addition to the general principles contained in the General Part of this Model, the Company ensures that the following principles are adhered to – also by adopting specific procedures.

1) Bookkeeping and preparation of the annual accounts

1. There is an obligation to act correctly, transparently and collaboratively, in accordance with applicable laws and established corporate practices, in all activities aimed at preparing the financial statements and other corporate communications, so as to ensure that shareholders and third parties are provided with a true and fair view of and correct information on the company's profit-and-loss, capital and financial position.

Within the scope of this activity, the following are expressly forbidden:

- representing or transmitting false, incomplete, or otherwise inaccurate data and information on the Company's profit and loss, balance sheet and financial position, for preparation and representation in the Company’s annual accounts, reports, prospectuses, or other corporate communications;
- omitting data and information required by law regarding the Company's profit and loss, balance sheet and financial position;
- returning contributions to shareholders or releasing them from the obligation to make such contributions, except in cases of legitimate capital reduction;
- distributing profits or advances on profits not actually earned or allocated by law to reserves;

2. the participation of multiple individuals is provided for in relation to bookkeeping and the preparation of the annual accounts, in order to ensure dual control (as a minimum) over the separate phases of these processes;

3. there is an obligation to ensure maximum traceability of each phase of the processes involved in the activities in question, to allow any errors/discrepancies to be readily identified;

4. there is an obligation to ensure a specific information flow to the SB concerning the key phases of the process of approving the financial statements, and also, where appropriate, to ensure opportunities for discussion between the SB and all parties involved in the process: the administration department, accountants, the Board of Directors, the Board of Statutory Auditors, and the audit firm.

2) Management of capital transactions and of Shareholder's Meeting activities

There is an obligation to strictly comply with all legal rules that safeguard the integrity and effectiveness of share capital, so as not to impair the guarantees of creditors and third parties in general. Within the scope of this activity, the following are expressly forbidden:

a) purchasing or subscribing for shares of the Company outside the cases envisaged by law, in violation of the integrity of share capital;
b) carrying out share capital reductions, mergers or demergers, n violation of legal provisions protecting creditors, causing them detriment;
c) forming and/or increasing fictitious share capital, attributing shares for a value lower than their nominal value during capital increases.

In the management of capital transactions, the following are ensured:

- identification of all obligations and deadlines provided by regulatory provisions;
- monitoring of all activities carried out by the various parties involved.

3) Management of dealings with control bodies

This activity includes the following sensitive processes: Preparation of the annual financial statements.

The management of dealings with the external audit firm is regulated as follows:

- the precise identification of the individuals responsible for receiving, collecting, consolidating, and transmitting data and information requested by the corporate bodies and by the audit firm, within the functions that are involved in Sensitive Processes, in compliance with the principle of segregation of duties;
- the provision of special control systems to ensure the origin and to verify the accuracy and completeness of the data, including through comparison with data and information contained in documents already communicated to said parties;
- the obligation to hold special meetings to share data and/or information transmitted, to ensure that such data and/or information are understood by the parties vested with control responsibilities, and the obligation to record the related resolutions;
- specific information flows between the functions involved in the process, and the documentation and traceability of the individual phases, with optimal collaboration and transparency;
- the obligation to provide - as completely, transparently, precisely, truthfully and promptly as possible - all data, information and documentation requested by the external auditor or by the Board of Statutory Auditors;
- criteria for selection of the external audit firm, and rules to maintain the independence of the external audit firm (or individual external auditor) during the mandate;
- formalisation of the outcomes of the main meetings held with audit firms (e.g., opening and closing meetings).

4) Share capital transactions: management of contributions, company assets, profits and reserves, equity and capital transactions

This activity includes the following Sensitive Processes: Preparation of the annual financial statements, management of corporate compliance formalities. The regulation of this activity requires:

- clear identification of roles and responsibilities as regards the evaluation of the transaction, preparation of documentation intended for the governing bodies;
- control of documentation accompanying resolutions of the governing bodies;

- existence of rules for managing the evaluation, authorisation, and management of capital transactions;
- archiving of resolutions and of related supporting documentation.

5) Communication, conduct, and recording of Shareholders' and Board of Directors meetings

This activity includes the following Sensitive Processes:

- management of corporate compliance formalities.

The regulation of this activity requires:

1. strict observance of legal and statutory provisions on the functioning of Shareholder's and Board of Directors meetings;
2. adoption and definition of formalised rules for the control of the exercise of voting rights and the gathering and exercise of voting proxies;
3. a clear and formalised corporate regime to identify roles and responsibilities involved in the transcription, publication, and archiving of Shareholders Meeting minutes.

CHAPTER B.6

Specific procedural principles governing Sensitive Processes pertaining to the offence of bribery/corruption among private individuals

In order to implement the rules listed in the previous Chapter, in addition to the general principles contained in the General Part of this Model, the Company ensures that the following principles are adhered to – also by adopting specific procedures.

1) Management of dealings with certification bodies

a. The Company establishes an authorisation and organisational system that:

i. defines the roles and responsibilities of the main functions involved in dealings with certification bodies, formally identifying in advance those who are responsible for managing dealings with them;
ii. ensures the traceability of contacts with such counterparts, to prevent any irregular conduct;

iii. guarantees, during inspections preparatory or prior to the issuance or confirmation of certifications, the presence of at least two individuals during all interactions with certifying officers (or, at least, during the final phase of the inspection, when the outcome of the inspection may be communicated verbally before being formalised in writing);

b. the Supervisory Body receives periodic as well as *ad hoc* information flows regarding the status of certifications, and any significant occurrences during the process of issuing or updating certifications.

2) Management of disputes and entering into settlement agreements

a. The Company adopts specific measures to determine:

i. the roles and responsibilities of individuals tasked with managing disputes and concluding settlement agreements;
ii. the conduct of prior periodic controls and checks to monitor the professionalism of consultants;
iii. the transparency and traceability of negotiation processes aimed at concluding settlement agreements;
iv. the tracking of the process of appointing external lawyers, ensuring that the related contracts include a Model 231 Clause;
v. the continuous monitoring of the dispute-management process (including pre-litigation phases), fulfilling the obligation to inform the relevant functions when such cases arise, and related actions taken, and defining the roles and responsibilities of each function in the resolution and management of disputes.

b. The Supervisory Body must be involved (if only for informational purposes) throughout the key phases of important disputes.

3) Management of dealings with lending institutions and insurance companies

1. A. The Company adopts specific measures:

i. to define the roles and responsibilities of the main functions involved in dealings with private financiers (banks or financial institutions) and insurance companies;
ii. to ensure the traceability of contacts with such counterparties, to prevent any irregular conduct.

2. The SB must be informed of any anomalies or problematic issues in dealings with lending institutions and insurance companies, and of any disputes arising in the context of such dealings;

3. the SB must also be informed of any significant insurance claims of particular relevance to the Company.

Specific procedural principles governing Sensitive Processes identified in connection with offences of bribery/corruption among private individuals

1) Selection and recruitment of personnel

a. The roles and responsibilities of internal functions involved in the personnel selection and recruitment process should be specifically identified, in compliance with the principle of role segregation and dual control;

b. the personnel selection and recruitment process should follow transparent criteria based on the following parameters:

i. the personnel selection and recruitment process should be structured across multiple phases, involving multiple functions/individuals;
ii. application of objective criteria – based on merit and professionalism – in choosing the most suitable candidate for recruitment and determining their work category and remunerations and contract terms;
iii. verification in advance of the absence of impediments to recruitment, and also of professionalism adequate to the candidate position or job duties in question;
iv. exclusion of any interference by third parties in the recruitment process of employees;
v. retention of documentation related to the selection process, also in order to facilitate its consultation by the Supervisory Body in the context of its oversight function;

c. any internal career advancements and awards (including the possible inclusion of a variable component in the remuneration, linked to the achievement of specific targets) must be granted according to objective criteria, based on merit and professionalism. In general, the Company does not tolerate unlawful conduct by employees aimed at achieving targets that result in rewards; in particular:

i. the grant of incentive payments such as bonuses should be based on the achievement of predetermined targets;
ii. career advancements should be evaluated based on professional qualifications and on the outcome of performance review meetings conducted with the function manager;

d. the Company guarantees that each new recruit:
i. receives an updated copy of the Company's Model when the employment relationship is created;
ii. signs a declaration of receipt and commitment to comply with the Model;
iii. receives, as part of the new recruit's initial training activities, foundational training on the legislation, principles and standards referenced in the Decree.

2) Management of gifts, donations and sponsorships

a) The Company adopts specific measures to regulate the purposes, methods, and limits for offering gifts and donations to third parties. This is to ensure that such offerings do not improperly influence or appear to improperly influence the beneficiary's independent judgment;

b) such gifts, free services or donations shall not, in general, exceed EUR 150.00 in value. Even if the relevant individuals come from countries where offering donations or gifts is a widespread courtesy practice, gifts should be appropriate, comply with legal provisions and should not be interpreted as a request for favours in return;

c) the Company has specific approval processes for permitted gifts or donations, as well as a list of acceptable gifts/donations;

d) any derogation from the safeguards in place for gifts or donations shall require the involvement of senior management, and shall be notified to the Supervisory Body;

e) a process is in place to evaluate requests for corporate gifts/sponsorships, aimed at ascertaining the credentials of the recipient;

f) the Company ensures that the Supervisory Body receives periodic reports (as provided for in the paragraph on information flows) on gifts, sponsorships and donations made during the reporting period.

3) Management of expense reimbursements

a) The Company establishes specific limits and procedures for reimbursing expenses incurred by company representatives and employees in the course of business activities;

b) all expense claims are recorded;

c) all travel and entertainment expenses incurred by the Company's staff and consultants must be supported by appropriate documentation and justified by their direct relevance to work activities;

d) expenses exceeding a certain threshold may only be reimbursed if pre-approved;

e) incurred expenses are reimbursed by reference to a traceable documentation trail.

4) Management of financial flows

a) The Company guarantees that individuals authorised to carry out any financial transaction are identified - in advance and retrospectively - by means of special powers of attorney that indicate their spending powers (providing for any approval thresholds based on expenditure amounts);

b) the Company's financial management tasks include formal and substantive checks on incoming and outgoing financial flows. These checks consider as a basis the counterparty's registered office and the destination or origin of the incoming or outgoing funds (e.g. so-called tax havens, countries on international blacklists, etc.);

c) the Company checks in advance that the payment recipient's account is not registered under a different name or located in a country other than where the recipient is based;

d) any increases in the price list already agreed with suppliers, and any different economic conditions such as discount percentages to be applied to year-end orders, must be communicated/agreed in writing (even in cases where no formal contract has been signed with the supplier);

e) it is expressly forbidden to make payments using non-traceable methods, except for small amounts (processed through the "petty cash" fund), which must nevertheless be duly authorised and documented;

f) before proceeding with payment, checks are conducted to ascertain whether services agreed with suppliers and consultants have actually been provided, and to ascertain the appropriateness of the price agreed;

g) the persons responsible for checking and overseeing compliance obligations associated with the aforementioned activities (e.g. invoice payments, allocation of funds obtained from the State or other bodies) must pay particular attention to implementing the said compliance

obligations, and immediately report any irregularities or problematic issues to the Supervisory Body.

5) Selection of suppliers and consultants, negotiation of related agreements and management of related relationships

a) All of the terms and conditions of all dealings between the company, suppliers and consultants shall be drawn up in writing, and those dealings shall comply with the provisions outlined in the paragraphs below (such relationships shall be governed by written agreements, at the very least the economic terms and conditions of the supply/consultancy relationship);

b) Suppliers and consultants shall be selected by reference to transparent processes - based on objective criteria that value merit and professionalism - and according to standardised procedures, which may involve competitive processes; alternatively, pre-approved parties may be used who have been included in a special vendors list (this document lists suppliers and consultants who have proven to be trustworthy and have had a long-standing relationship with the Company, as outlined below);

c) the Company ascertains the professionalism and integrity of suppliers and consultants at the initial recruitment stage and periodically thereafter, requiring them to inform the Company, in good time, of any loss of such qualifications (e.g. in the event of a conviction for an offence under the Decree);

d) the Company formalises a 'vendor list' of trustworthy suppliers whom it uses periodically, which indicates the supplier's name and annual turnover, and the key formalities adopted within the commercial relationship in question (e.g. whether a fixed rate is used or prices are negotiated case by case, whether purchase orders are used or a supply contract has been signed);

e) contracts with suppliers and consultants must include Model 231 Clauses;

f) where relationships with suppliers/consultants are already in place or cannot be regulated by a formal written contract, the Company sends suppliers/consultants a "231 Notice", requesting their signature, which includes the Model 231 Clauses referred to in the previous paragraph.

CHAPTER B.7

Controls by the Supervisory Body

B.7.1 SB Control in general

The SB conducts periodic checks to verify that Recipients, within the limits of their respective duties and responsibilities, properly observe the rules and principles enshrined in this Special Part and in the company procedures to which that Part explicitly or implicitly refers.

In particular, it is the responsibility of the SB:

- to monitor the effectiveness of the procedural principles provided therein, or the principles contained in company policies adopted for the prevention of offences outlined in this Special Part;
- to propose any necessary changes to Sensitive Processes attributable to potential changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The SB shall be promptly informed of any infringements of the specific procedural principles contained in this Special Part, or of infringements of company procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART - C -

Crimes of receiving stolen goods, money-laundering, use of money, goods or assets of illicit origin, as well as self-laundering, financing of terrorism and crimes involving non-cash payment instruments

CHAPTER C.1

This Special Part refers, respectively, to the criminal offences of money laundering introduced into the Legislative Decree 231/2001 (Article 25-octies), through the Legislative Decree 231/2007 ('*Anti-Money Laundering Decree'*), and also to the terrorism-related offences (in particular, the financing of terrorism) provided for under Article 25-quater of Legislative Decree 231/2001, and to the criminal offences committed using non-cash payment instruments introduced under Article 25-octies.1 of the latter Decree, taking into account the similarity of corporate safeguards aimed at preventing both types of offences.

C.1.1. Crimes of receiving stolen goods, money laundering, use of money, goods or economic benefits of illicit origin, and self-laundering (Art. 25-octies of Legislative Decree 231/2001)

With regard to this Special Part, the below is a list of the offences specified in Article 25-octies of the Decree, relating to receiving, money laundering, use of money, goods, or other economic benefits of illicit origin and, finally, self-laundering which was introduced by Law 186/2014 and classified under Article 648-ter.1 of the Penal Code.

The precondition of the four types of offences is the same: the illicit origin of the money or other economic benefit received by the perpetrator, and full knowledge of such origin. Self-laundering consists of the activity of concealing proceeds derived from one's own crimes; it is mainly found in connection with specific criminal offences such as tax evasion, corruption, and misappropriation of company assets. Regarding the liability of entities for all the aforementioned offences, the legislature has provided for a system of aggravating circumstances in addition to the application of disqualification measures.

RECEIVING STOLEN GOODS (ART. 648 OF THE PENAL CODE)

This offence is committed by any person who, in order to obtain a profit or proceeds for themselves or others, purchases, receives or conceals money or items derived from any criminal offence (*delitto*) or misdemeanour (*contravvenzione*), or becomes involved in their acquisition, receiving or concealment.

'*Purchase*' refers to the effect of a business transaction, whether for valuable consideration or otherwise, by which the agent gains possession of the item in question.

'*Receiving*' refers to any form of obtaining possession of the item derived from the criminal offence, even if only temporarily.

'*Concealment*' refers to the hiding of the item derived from the criminal offence after it has been received.

For the offence to be committed, it is not necessary for the money or goods to come directly or immediately from a crime; an indirect origin is sufficient, provided the agent is aware of such origin. The offence therefore applies not only to the product or profit or proceeds of the criminal offence, but also to the money or items that constitute the price of the crime i.e. to the items that are purchased using money of illicit origin or money obtained from the sale of items of illicit origin (for example, if a company, in order to obtain a favourable price, purchases goods from a person who, alongside supplying such goods, is known to engage in illegal activities such as drug trafficking or is part of a mafia-type association and uses the profits from such illegal activities to invest in legitimate business).

MONEY LAUNDERING (ART. 648-BIS OF THE PENAL CODE)

This offence is committed where a person substitutes or transfers money, goods or other economic benefits derived from a crime or misdemeanour, or carries out other transactions in respect of such money, goods or assets, in such a way as to hinder the identification of their illicit origin.

'*Substitution*' refers to the act of replacing money, goods or other economic benefits of illicit origin with different assets.

'*Transfer*' refers to the act of "*cleaning*" money, goods or other economic benefits of illicit origin by engaging in business transactions.

For this offence, therefore, an extra step is required beyond the offence of receiving, namely, acts are carried out to ensure the substitution of the money.

USE OF MONEY, GOODS OR ECONOMIC BENEFITS OF ILLICIT ORIGIN (ART. 648-TER OF THE PENAL CODE)

This offence is committed when money, goods, or other economic benefits derived from a crime or misdemeanour are used in economic or financial activities.

Only persons are punishable for this offence who are not already accomplices in the principal offence or who are not liable for receiving or money laundering.

The term '*use'* is generally synonymous with '*utilisation for any purpose'*. However, since the legislature's ultimate aim is to prevent the disruption of the economic system and of competitive equilibrium by the use of illegitimate capital available at lower cost than legitimate capital, it is considered that '*use'* should in fact be understood as '*investment'*. Therefore, only use for profit-making purposes should be considered relevant.

Note that the common premise of all three criminal offences under Articles 648, 648-bis, and 648-ter of the Penal Code is the illicit origin of the money or economic benefit that has come into the agent's possession. These offences are, however, distinguished by their subjective elements: the first requires, in addition to awareness of the illicit origin (which is necessary for all three), only a general intent to profit or gain, while the second and third require the specific

intent to obscure the illicit origin, with the additional peculiarity, in the case of the third criminal offence, that this intent must be pursued through the use of the resources in economic or financial activities.

The penalty is increased if the criminal offence is committed in the course of professional activity.

SELF LAUNDERING (ART. 648-TER(1) OF THE PENAL CODE)

Article 648-ter.1 of the Penal Code provides for the punishment of anyone who, '*having committed or contributed to the commission of a criminal offence, uses, substitutes or transfers - in economic, financial, business or speculative activities - money, goods or other economic benefits obtained from the commission of that criminal offence, in a manner that concretely hinders the identification of their illicit origin'*. A specific penalty is also provided '*when the criminal act concerns money or items derived from a misdemeanour (contravvenzione) punishable by a term of imprisonment exceeding one year at the maximum or six months at the minimum'.*

The second paragraph of Article 648-ter.1 of the Penal Code also provides for a mitigating circumstance if the money, goods, or other economic benefits derive from a criminal offence for which the maximum penalty is less than five years' imprisonment.

This offence, therefore, punishes conduct whereby the perpetrator, after committing or contributing to a crime, seeks to '*concretely hinder the identification of the illicit origin'* of the proceeds obtained from the initial crime by reusing them '*in economic, financial, business or speculative activities'.*

Aggravating circumstances include:

- committing the offence in the manner described in Article 416-bis of the Penal Code, on the offence of '*Domestic or foreign mafia-type criminal associations'*, or with the aim of facilitating the activities of mafia-type associations. In such cases, the penalties provided for in the first paragraph of Article 648-ter.1 of the Penal Code will be applicable;
- committing this offence in the course of banking, financial, or other professional activities.

A mitigating circumstance – which results in a reduction of the penalty by up to half – applies if the offender '*has taken effective steps to prevent the conduct from leading to further consequences, or to secure evidence of the crime and the identification of the goods, money and other economic benefits originating from the crime' (Article 648-ter.1, paragraph VI, of the Penal Code).*

However, the offence of self-laundering is not punishable under Article 648-ter.1 of the Penal Code where the money, goods, or other economic benefits are intended '*for mere personal use or enjoyment'.*

C.1.2. Offences of Financing Terrorism

Among the offences of facilitating terrorism, the only ones that could, in theory, potentially be of relevance within the Company involve the '*financing of conduct aimed at terrorism'* (Article 270-quinquies.1 of the Penal Code).

Under Article 270-quinquies.1 of the Penal Code, the financing of conduct that has terrorist purposes refers to any activity aimed at collecting, depositing, holding or disbursing funds or economic resources, in any manner, which are intended to be used, in whole or in part, to commit one or more criminal offences with terrorist aims or, in any case, with aims that are directed at facilitating the commission of one or more criminal offences with terrorist purposes as defined by the Italian Penal Code, regardless of whether the funds or economic resources are actually used to commit such offences.

C.1.3. Crimes involving non-cash payment instruments

MISUSE AND FALSIFICATION OF NON-CASH INSTRUMENTS (ART. 493-TER OF THE PENAL CODE)

Article 493-ter of the Penal Code punishes anyone who, with the aim of obtaining a profit for themselves or others, illegitimately uses - not being the owner/holder thereof - credit or payment cards or any other similar document enabling the withdrawal of cash or the purchase of goods or the provision of services, or any other non-cash payment instrument.

The first paragraph of the provision also punishes anyone who, with the aim of obtaining a profit for themselves or others, falsifies or alters such instruments or documents or possesses,

transfers or acquires such instruments or documents that are of illicit origin or are otherwise falsified or altered, as well as payment orders produced with them.

POSSESSION AND DISTRIBUTION OF COMPUTER EQUIPMENT, DEVICES OR PROGRAMS IN ORDER TO COMMIT OFFENCES INVOLVING NON-CASH PAYMENT INSTRUMENTS (ART. 493-QUATER OF THE PENAL CODE)

Under Article 493-quater of the Penal Code, unless the act constitutes a more serious offence, any person is punishable who - with the aim of using them or enabling others to use them in the commission of offences involving non-cash payment instruments - produces, imports, exports, sells, transports, distributes, makes available or in any way procures for themselves or others computer equipment, devices or programs that, by their technical-construction or design characteristics, are primarily intended for committing such offences or are specifically adapted for the same purpose.

COMPUTER FRAUD (ART. 640-TER OF THE PENAL CODE)

The offence of computer fraud is committed when, with the aim of obtaining an unjust profit for themselves or others, the perpetrator unlawfully alters the functioning of a computer system or interferes, without authorisation, with data, information or programs contained in a computer system.

The offence of computer fraud is referenced in Article 25-octies.1 with regard to the aggravated case provided for in the second paragraph of Article 640-ter of the Penal Code ('if the act results in a transfer of money, monetary value or virtual currency or is committed with abuse of one's status as a system operator').

FRAUDULENT TRANSFER OF ASSETS (ARTICLE 512-BIS OF THE PENAL CODE)

The offence of fraudulent transfer of assets is committed when the ownership or availability of money, goods, or other economic benefits is fictitiously attributed to others with the aim of circumventing legal measures combating the acquisition and use of monies of illicit origin or smuggling, or of facilitating the commission of an offence pursuant to Articles 648, 648-bis, or 648-ter of the Penal Code.

CHAPTER C.2

C.2.1 Sensitive Processes in the context of the criminal offences of receiving stolen goods, money laundering, use of money, goods or economic benefits of illicit origin as well as self-laundering and financing of terrorism

The following are the main Sensitive Processes of relevance to the offences under consideration, which the Company has identified within its organisation:

1. selection of suppliers and consultants, negotiation of related agreements and management of related relationships;
2. management of financial flows;
3. purchase of goods and raw materials;
4. management of tax compliance obligations;
5. investment activities and special transactions.

CHAPTER C.3

General Principles of Conduct

The aim of this Special Part, with a view to preventing the commission of the offences considered herein, is that all Recipients of the Model should adhere to all procedures and principles that are directly or indirectly instrumental to the prevention of money laundering, adopted by the Company as a basic way of ensuring its smooth operation, reliability, and reputation.

In particular, the aforementioned individuals, also depending on the type of relationship with the Company, must adhere to the following principles of conduct:

1. to refrain from engaging in conduct that constitutes an offence under this Special Part;
2. to refrain from engaging in conduct that, while not constituting an offence per se, could potentially become one;
3. to act and conduct oneself correctly, transparently and collaboratively, in compliance with legal norms and internal company procedures, in all activities aimed at managing the master file records of suppliers, clients, or Italian or foreign contractual counterparties;
4. not to engage in business dealings with natural or legal persons known or suspected of belonging to criminal organisations or otherwise operating outside of the law;

5. not to use anonymous instruments to transfer significant sums of money;
6. to constantly monitor company financial flows.

In order to prevent the commission of the offence of self-laundering, the following is forbidden:

1. issuing invoices or other accounting documents for transactions that are wholly or partially non-existent;
2. issuing invoices or other accounting documents for payments exceeding the actual amounts;
3. making payments against invoices for services not in fact received.

The following obligations must also be observed:

1. the Company regulates interactions between all parties involved in the drafting of accounting (including financial statements) and tax returns, by carefully specifying individual roles;
2. the Company ensures the proper and orderly keeping of accounting records and other documents whose retention is required for tax purposes;
3. the Company oversees the periodic monitoring of compliance with principles governing the drafting, keeping and storage of accounting declarations.

CHAPTER C.4

C.4.1. Specific procedural principles

When engaged in the Sensitive Processes identified in this Special Part, the Company – also by adopting specific procedures – ensures that the following principles are respected.

1) Selection of suppliers and consultants, negotiation of related agreements and management of related relationships

a) All of the terms and conditions of all dealings between the company, suppliers and consultants shall be drawn up in writing, and those dealings shall comply with the provisions outlined in the paragraphs below (such relationships shall be governed by written agreements, at the very least the economic terms and conditions of the supply/consultancy relationship);

b) Suppliers and consultants shall be selected by reference to transparent processes - based on objective criteria that value merit and professionalism - and according to standardised procedures, which may involve competitive processes; alternatively, pre-approved parties may be used who have been included in a special vendors list (this document lists suppliers and consultants who have proven to be trustworthy and have had a long-standing relationship with the Company);

c) the Company ascertains the professionalism and integrity of suppliers and consultants at the initial recruitment stage and periodically thereafter, requiring them to inform the Company, in good time, of any loss of such qualifications (e.g. in the event of a conviction for an offence under the Decree);

d) the Company formalises a so-called vendor list of loyal suppliers whom it uses periodically, which indicates the supplier's name and annual turnover, and the key formalities adopted within the commercial relationship in question (e.g. whether a fixed rate is used or prices are negotiated case by case, whether purchase orders are used or a supply contract has been signed, also one that is automatically renewable);

e) contracts with suppliers and consultants must include Model 231 Clauses;

f) where relationships with suppliers/consultants are already in place or are not regulated by a formal written contract, the Company sends the suppliers/consultants a '231 Notice', requesting their signature, which includes the Model 231 Clauses.

2) Management of financial flows

a) The Company guarantees that individuals authorised to carry out any financial transaction are identified - in advance and retrospectively - by means of special powers of attorney that specify their spending powers (including any approval thresholds based on expenditure amounts);

b) the Company's financial management tasks include formal and substantive checks on incoming and outgoing financial flows. These checks consider as a basis the counterparty's registered office and the destination or origin of the incoming or outgoing funds (e.g. so-called tax havens, countries on international blacklists, etc.);

c) the Company checks in advance that the payment recipient's account is not registered under a different name or located in a country other than where the recipient is based;

d) any increases in the price list already agreed with suppliers, and any different economic conditions such as discount percentages applicable to orders, must be communicated/agreed in writing (even in cases where no formal contract has been signed with the supplier);

e) it is expressly forbidden to make payments using non-traceable methods, except for small amounts (processed through the 'petty cash' fund), which must nevertheless be duly authorised and documented;

f) before proceeding with payment, checks are conducted to ascertain whether services agreed with suppliers and consultants have actually been provided, and to ascertain the appropriateness of the price agreed;

g) the individuals responsible for checking and overseeing compliance obligations associated with the aforementioned activities (e.g. invoice payments, allocation of funds obtained from the State or EU bodies, etc.) must pay particular attention to implementing the said compliance obligations, and immediately report any irregularities or problematic issues to the Supervisory Body.

3) Purchase of goods and raw materials

The Company, in the purchase of any goods (machinery, products, tools, general items) and raw materials, pays particular attention to ensuring that:

i. such goods and raw materials come only from regular channels (authorised Suppliers);
ii. the quantity and quality of goods purchased with each order are correctly accounted for.

4) Management of tax compliance obligations

a) When drafting annual income tax and VAT declarations, the Company adopts formal safeguards to ensure that:

- asset items must not be itemised for an amount less than the actual amount, nor may fictitious liability items be itemised;
- a taxable base lower than the applicable one must not be indicated;
- the deadlines set by applicable legislation for their submission and the subsequent payment of resultant taxes must not be unnecessarily delayed.

b) The Company undertakes to ensure that certificates issued, or otherwise due, as withholding agent correspond with the actual payment of the withholdings;

c) The Company also undertakes to ensure that the principle of segregation of roles is reflected in the management of company accounts and in the subsequent transposition into tax returns (for example, by verifying the accuracy of declarations against accounting records).

5) Investment activities and special transactions

a) When carrying out any investments and/or special transactions, the Company undertakes to ensure:

i. their consistency with the corporate purpose;
ii. the adoption of transparent and traceable methods for all phases of the process and for the money movements involved;
iii. the involvement (if only for informational purposes) of the Supervisory Body in relation to significant investments and any special transaction;

b) the Company ensures the transparency and traceability of any agreements/joint ventures with other companies to realise investments, in Italy and abroad, and verifies their economic adequacy (observing average market prices, also with the support of trusted professionals).

CHAPTER C.5

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the scope of their respective duties and responsibilities, comply with the rules and principles set out in this Part.

In particular, the SB is tasked with the following:

- monitoring the effectiveness of internal procedures/rules on the prevention of offences of receiving, money laundering, and use of money, goods or economic benefits of illicit origin, as well as self-laundering and financing of terrorism;
- proposing any necessary changes to Sensitive Processes attributable to changes in the Company's operations;
- reviewing special reports received from audit/control bodies, from third parties or from any key corporate officer, conducting any necessary or appropriate investigations in relation to the reports received.

The SB shall be promptly informed of any infringements of the specific procedural principles contained in this Special Part, infringements of company procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART – D –

Criminal offences of manslaughter and serious or grievous injury committed in violation of workplace health and safety rules

CHAPTER D.1

D.1.1. Offences committed in infringement of applicable workplace health and safety prevention rules (Art. 25-septies, Legislative Decree 231/2001)

A brief description of the offences committed in violation of the rules on health and safety at work, indicated in Article 25-septies of the Decree, is provided below.

This article, originally introduced by Law no. 123 of 3 August 2007 and subsequently replaced pursuant to Article 300 of the Consolidated Safety Act, envisages the imposition of monetary penalties and disqualification sanctions on entities whose representatives commit offences under the Penal Code Article 589 (manslaughter) and Article 590 III (culpable serious or grievous personal injury committed while violating workplace health and safety rules).

Note the one essential and unifying element of the various possible forms of employer liability, for the purposes of application of Article 25-septies of Legislative Decree 231/2001, is the failure to adopt all safety and prevention measures technically possible and practically implementable, based on experience and on cutting-edge technical-scientific knowledge.

To ensure that effective safeguards are put in place against the commission of offences under Article 25-septies of the Decree, the Company has decided to adopt this Special Part, in compliance with the provisions of Article 30 of the Consolidated Safety Act.

MANSLAUGHTER (ARTICLE 589 OF THE PENAL CODE)

This offence is committed whenever a person causes the death of another through negligence.

The conduct relevant to this Special Part is described in Article 589, paragraph II of the Penal Code, which establishes an aggravating circumstance for the offence of manslaughter. This circumstance applies not only when a violation of specific workplace accident prevention rules is alleged, but also where the conduct is contrary to Article 2087 of the Italian Civil Code, which imposes a specific obligation on the employer to eliminate any hazardous situation that could result in an injurious event.

CULPABLE SERIOUS OR GRIEVOUS PERSONAL INJURY (ART. 590 PARA. 3 OF THE PENAL CODE)

This offence is committed whenever a person, in violation of workplace accident prevention rules, causes another individual serious or grievous personal injury through negligence.

Under Article 583(I) of the Penal Code, harm is deemed serious in the following cases:

1) *'If the act results in an illness that endangers the life of the victim, or an illness or inability to perform normal activities for more than forty days;*
2) *if the act causes permanent impairment of a bodily sense or organ'.*

Under Article 583(2) of the Penal Code, harm is considered grievous if the act results in:

- *'An illness/disease that is certainly or probably incurable;*
- *the loss of a bodily sense;*
- *the loss of a limb, or a mutilation which renders the limb unusable, or loss of the use of an organ or of the ability to procreate, or a permanent and serious speech impairment;*
- *the deformity or permanent disfigurement of the face'.*

CHAPTER D.2

D.2.1. Sensitive Processes in relation to offences of manslaughter and serious or grievous injury committed in violation of workplace health and safety rules

All corporate areas are potentially at risk of non-compliance with the requirements of workplace safety rules. Therefore, importance is attributed to the verification of compliance with workplace health and hygiene rules, and to the establishment of information-related procedures for managing facilities and assessing workplace health conditions.

The company work environment is thus deemed to be exposed to ongoing workplace safety risks, based on the nature of the activity carried out.
With this in mind, the following Sensitive Processes can be identified:

- risk assessment activities;
- health surveillance;
- outsourcing of works to third parties inside Company premises;
- emergency management (first aid, fire safety, etc.);
- organisational aspects - delegated powers, appointment of the Risk Prevention and Protection Service Manager (RSPP) and the Workers' Safety Representative (RLS), budget and expenses);
- provision of training/information to personnel.

Due to the high levels of risk, information and training in the area of workplace safety is provided to the entire organisation on an ongoing basis. To this end, all company functions are involved in managing the process of implementing Legislative Decree 81/2008, each within their own respective remits, but also informing the entire organisation in view of the particular application of the law.

CHAPTER D.3

D.3.1 General principles of conduct relevant to workplace health and safety offences

In order to ensure the implementation of principles aimed at protecting the health and safety of workers as identified in Article 15 of the Consolidated Safety Act, and in compliance with Articles 18, 19, and 20 of the same decree, the following is established.

Company safety policy

The Company's health and safety policy must seek to enumerate the principles that guide all Company actions, to which all Recipients must adhere by reference to their role and responsibilities within the Company, with a view to the health and safety of all workers.

This policy must include:

- a clear statement of that entire company organisation has responsibility in managing health and safety at work, each Recipient according to their specific duties and competencies;
- a commitment to consider these issues as an integral part of the company management; a commitment to continuous improvement and prevention;
- a commitment to provide the necessary human and instrumental resources;
- a commitment to ensure that Recipients, within the scope of their responsibilities, are sensitised to carry out their activities in compliance with applicable health and safety regulations;
- a commitment to periodically review the health and safety policy adopted, in order to ensure that it continues to be adequate to the Company's organisational structure.

With regard to health and safety at work, GIMA has established an organisational structure in line with the current prevention regime, aiming to eliminate or, where this is not possible, reduce and manage risks to workers. Tasks and responsibilities in the field of workplace health and safety have also been defined, from the employer right down to the individual worker.

To familiarise oneself with the general principles of conduct, the reader may consult the General Risk Assessment Document drawn up pursuant to Legislative Decree 81/08, and also all internal workplace safety procedures.

Duties and responsibilities

When defining the organisational and operational duties of workers, it is essential to clearly specify and make known the safety-related responsibilities that fall within their remit, including inspection, verification, and surveillance duties in the workplace health and safety field.

The assignment of duties and responsibilities lies exclusively with the employer, within the limits provided for by law.

Risk Prevention and Protection Service Manager (RSPP):

- this figure must be formally appointed;
- specific requirements for this role, in line with legal provisions, are defined based on the scope of the activity;
- checks on compliance with legal requirements must be documented and traceable;
- the RSPP's (Prevention and Protection System Manager) formal acceptance of their appointment must be documented and traceable.

Risk Prevention and Protection Service (SPP):

- this figure must be formally appointed;
- specific requirements for this role, in line with legal provisions, are defined based on the scope of the activity;
- checks on compliance with legal requirements must be documented and traceable;
- the SPP staff's formal acceptance of their appointment must be documented and traceable.

Company medical officer:

- checks on compliance with legal requirements must be documented and traceable;
- relevant health and risk documentation must be prepared in accordance with applicable regulations;
- the company medical officer's formal acceptance of their appointment must be documented and traceable.

Emergency appointees:

- workers responsible for implementing emergency, fire prevention, and first aid measures as required under applicable rules must be formally appointed;
- specific requirements for this role, in line with legal provisions, are defined based on the scope of the activity;
- checks on compliance with legal requirements must be documented and traceable;

- the appointee's formal acceptance of their appointment must be documented and traceable.

CHAPTER D.4

D.4.1 Specific procedural principles relevant to workplace health and safety offences

Recipients of this Model shall refrain from engaging in conduct that may constitute an offense pursuant to Article 25-septies of the Decree, or from engaging in conduct that, individually or collectively and directly or indirectly, may trigger the offences described therein.

When engaged in the Sensitive Processes identified in this Special Part, the Company – also by adopting specific procedures – ensures that the following principles are respected.

1) Management of Obligations under the Consolidated Safety Act

The Company complies with the provisions of the Workplace Health and Safety Consolidation Act, referenced in Legislative Decree 81/08. To this end, the Company has drafted a Risk Assessment Document (DVR), which identifies risks to the health and safety of workers, sets out a series of tools and prevention criteria in order to provide personnel with safeguards and information, and ensures that protective equipment or devices are continuously updated. The Model fully incorporates the provisions of the Risk Assessment Document adopted by our Company. The Company guarantees the periodic participation of personnel in workplace safety training courses.

In order to prevent occupational accidents, illnesses and diseases, the Company:

1. promptly complies with applicable legal provisions in the field of workplace health and safety;
2. ensures that meetings under Article 35 of the Consolidated Safety Act are convened at least once a year and that the employer or a specially delegated representative participates;
3. ensures that, where appropriate, functions are delegated in the health and safety field. The delegated power, which must be adequately publicised, must:
   i. be evidenced by a written document with date certain;
   ii. be formally accepted by the delegatee, who needs to satisfy all the professionalism and experience criteria required by the specific type of functions delegated;

iii. grant the delegatee all organisational, management, and control powers, as well as the degree of spending autonomy required by the specific nature of the functions delegated;

4. provides adequate information and training to employees and to all those who work at the Company's offices, on the specific risks inherent in the company, however limited, and on the consequences of those risks and the prevention and protection measures adopted;

5. stores documentation related to health and safety management in the workplace;

6. ensures the periodic monitoring of prevention and protection measures adopted in the workplace. In particular, there must be periodic monitoring of the following: i.) preventive and protective measures established for health and safety management in the workplace; ii.) the adequacy and functionality of such measures;

7. plans - based on the results of the monitoring activities - the necessary interventions to eliminate critical issues identified: this is to ensure that the health and safety system is adequately implemented and the set objectives are achieved;

8. establishes periodic information flows between the Supervisory Body and those who are involved in processes deemed sensitive in the context of health and safety offences.

CHAPTER D.5

Controls by the Supervisory Body

Subject to the Supervisory Body's discretionary power to initiate specific checks following reports received (see the General Part of this Model for further detail), the SB Body may:

1. participate in meetings that the Company may organise between functions responsible for workplace health and safety, assessing which of these are relevant for the proper performance of its duties;

2. access all relevant company documentation available.

The Company also establishes information flows to the SB so that it may obtain information enabling it to monitor accidents and critical issues and information about any confirmed or suspected occupational diseases.

The SB must be promptly informed of any violations of the specific procedural principles contained in this Special Part or of the company procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

The SB, when performing the above activities, may use all qualified resources within the company (e.g. the Risk Prevention and Protection Service Manager (RSPP); the workers' safety representative; the company medical officer; those responsible for implementing emergency and first aid measures).

SPECIAL PART - E -

Computer offences and copyright infringement offences

CHAPTER E.1

E.1.1. Computer offences (Art. 24-bis of Legislative Decree 231/01) and copyright infringement offences (Art. 25-novies of Legislative Decree 231/01)

This Special Part refers to computer offences (Article 24-bis), and also to the copyright infringement offences which Law 99/2009 included among the predicate offences punishable under Legislative Decree 231 (Article 25-novies).

The Law 90/2024, '*Provisions on the strengthening of national cybersecurity and on computer offences '(*also known as the '*Cybersecurity Law*'), introduced new provisions to enhance cybersecurity in the Italian legal system. This law impacts the administrative liability of entities under the Decree, as it modifies various aspects of the predicate offence indicated in Article 24-bis '*Computer offences and illegal data processing'*.

Firstly, the first paragraph of Article 24-bis of the Decree has seen a general increase in the financial penalties imposed on entities for the commission of computer offences contemplated therein, now ranging from 500 to 700 units, compared to the previous range of 100 to 200 units.

In the second paragraph of Article 24-bis, references to Article 615-quinquies ('*Unauthorised possession, dissemination and installation of equipment, devices or programs aimed at damaging or disrupting a computer or electronic telecommunications system"',* repealed by Law 90/2024, have been removed and replaced by Article 635-quater.1 '*Damaging computer*

or electronic telecommunications systems', whose provisions are nevertheless comparable, albeit intensified by the inclusion of two new aggravating circumstances.

Finally, a new paragraph (I-bis) has been inserted, incorporating a new offence introduced into the Penal Code by Law 90/2024: extortion through computer offences (Art. 629, paragraph III, Penal Code), which is accompanied by a monetary penalty of *300 to 800 units* and by the disqualification sanctions indicated in Art. 9, paragraph II, of Legislative Decree 231/2001, applicable for a duration of not less than two years.

Lastly, the application of the disqualification sanction under Article 9 was also extended to the offence provided for in the new paragraph I-bis.

That said, a description is given below of the individual offences provided for in Articles 24-bis and 25-novies of the Decree, which are relevant to GIMA (if only in theory). Note, here, that although the two types of offences safeguard different legal interests, it was deemed appropriate to address them in a single Special Part because:

- both offences presuppose the correct use of IT resources;
- the Sensitive Processes are, by virtue of this circumstance, partially overlapping;
- the principles of conduct aim, in both cases, to ensure that Recipients are fully aware of the multiple consequences arising from the improper use of IT resources.

E.1.2. Computer offences

FALSIFICATION IN ELECTRONIC DOCUMENTS (ARTICLE 491-BIS OF THE PENAL CODE)

This article establishes that all offences of falsification of documents (including false statement by a public official and material falsification in a public instrument), are punishable even if the conduct relates to an electronic (i.e. computer) document and not a paper document.

Electronic documents are therefore fully equated to traditional documents.

An electronic document should be understood as a digital representation of documents, acts, facts or data of legal relevance (Art. 1, paragraph I, letter p, Legislative Decree 82/2005, as amended).

For example, the offence of falsification in electronic documents is committed by fraudulently entering false data into public databases or where, for example, a worker responsible for managing electronic documents deliberately modifies data so as to falsify it.

This offence could also be committed, for example, by erasing or altering information of probative value present on company systems, with the aim of eliminating evidence of a different offence.

UNAUTHORISED ACCESS TO A COMPUTER OR ELECTRONIC COMMUNICATIONS SYSTEM (ART. 615-TER OF THE PENAL CODE)

This offence is committed when a person '*gains unauthorised access to a security protected computer or electronic communications system or who maintains such access against the express or implied will of the person entitled to exclude them'.*

The offence is punishable by a term of imprisonment up to three years.

The penalty is increased to between two and ten years:

1) if the act is committed by a public official or public service officer, by abusing their powers or violating the duties inherent in their function or service, or by anyone who works lawfully or unlawfully as a private investigator, or by abusing their role as a system operator;

2) if the perpetrator uses threats or violence against property or persons, or is visibly armed;

3) if the act results in the destruction or damage of the system, the total or partial disruption of its functioning, or the destruction or damage or removal (including simply by reproduction or transmission) of any data, information or programs contained within it, or by rendering said information or programs inaccessible to the data owner.

If the acts referred to the first and second subsections relate to computer or electronic communications systems of military interest or concern public order, public safety, public health or civil defence, or if they concern the public interest in general, the punishment shall be a term of imprisonment between three and ten years and between four and twelve years, respectively.

The offence of unauthorised access to a computer system falls within the category of crimes against individual freedom. The interest that is protected under the law is that of the "computer domicile," although some argue that the protected interest is instead the integrity of the data and programs contained in the computer system. The access is unauthorised because it contravenes the will of the system owner, which is implicitly manifested by the system owner having implemented safeguards that prevent third parties from accessing the system.

The offence of unauthorised access to a computer system is also committed where a person, who has legitimately gained access to the system, remains in the system against the system owner's wishes, or by a person who uses the system for purposes other than those for which they were authorised.

For example, the offence is committed when a person gains unauthorised access to a computer system and prints out a document contained in another person's PC storage, even if no files are removed, simply by making a copy (unauthorised access for copying) or simply by viewing information (unauthorised access for viewing).

The offence could, in theory, be committed by any employee of the Company who gains unauthorised access to third-party computer systems (outsider hacking), for example, in order to view or obtain confidential data of a competitor, or by manipulating data present on corporate systems as a result of business processes in order to produce a false financial statement or, finally, by gaining unauthorised access to company systems which the users of those systems have protected by security measures, in order to activate services that customers have not requested.

UNAUTHORISED POSSESSION, DISSEMINATION AND INSTALLATION OF EQUIPMENT, CODES AND OTHER MEANS TO ACCESS COMPUTER OR ELECTRONIC TELECOMMUNICATIONS SYSTEMS (ART. 615-QUATER OF THE PENAL CODE)

This offence is committed by anyone who, '*in order to obtain a benefit for themselves or others or to cause detriment to another party, unlawfully procures, holds, produces, reproduces, disseminates, imports, communicates, delivers or otherwise makes available to others, or installs, appliances, devices, instruments, parts of devices or instruments, codes, passwords or*

other means suitable for accessing a computer or electronic communications system protected by data security measures, or who provides instructions or information for such purpose'.

The legislature introduced this offence to prevent cases of unauthorised access to computer systems. Article 615-quater of the Penal Code, therefore, criminalises actions that are preparatory to unauthorised access, as they involve procuring for oneself or others the means of access needed to bypass a computer system's security barriers.

Devices that enable unauthorised access to a computer system include, for example, codes, passwords, or computer cards (badges, credit cards, ATM cards and smart cards).

This offence is committed when a person who legitimately possesses the aforementioned devices (system operator) communicates them without authorisation to third parties, and also when such a person unlawfully obtains one of these devices. The conduct is unauthorised and illicit if the access codes are obtained in violation of a rule or contractual clause that prohibits such conduct (e.g. an Internet policy).

Article 615-quater also punishes those who provide instructions or information enabling one to reconstruct the access code or bypass security measures.

For example, the offence of unauthorised dissemination of access codes would be committed by a Company employee who has lower-level access clearance to a computer system, if they unlawfully obtain a higher level of access by procuring codes or other access means through the exploitation of their position in the Company, or by obtaining the access code fraudulently or deceptively.

ILLEGAL INTERCEPTION, BLOCKING OR DISRUPTION OF COMPUTER OR ELECTRONIC COMMUNICATIONS (ART. 617-QUATER OF THE PENAL CODE)

This offence is committed when a person, with the aim of benefiting themselves or others or causing detriment to others, fraudulently intercepts communications available on a computer or electronic telecommunications system or between multiple systems, or obstructs or disrupts such communications, or when a person discloses the content of the communications to the public, partially or entirely, through any public information channel.

The provision safeguards the freedom and confidentiality of computer or electronic communications during the transmission phase, in order to ensure the authenticity of their content and the confidentiality thereof.

The fraudulent element lies in the covert manner of the interception, done without the knowledge of the person sending or receiving the communication.

For this offence to be committed, the communication must be current i.e. underway, and personal, i.e. directed to a specific or identifiable number of individuals (natural or legal persons). If the communication is directed to an indeterminate number of individuals, it will be deemed to be directed towards the public.

Using techniques of interception, it is possible, while data is being transmitted, to gain knowledge of the content of communications between computer systems or to alter their destination: the typical aim of such actions is to violate the confidentiality of messages, compromise their integrity, or to delay or prevent their arrival at the intended destination.

The offence is committed, for example, if an employee carries out industrial sabotage by fraudulently intercepting the communications of a competitor, which benefits the entity itself.

UNAUTHORISED POSSESSION, DISSEMINATION AND INSTALLATION OF EQUIPMENT AND OTHER MEANS TO INTERCEPT, BLOCK OR DISRUPT COMPUTER OR ELECTRONIC COMMUNICATIONS (ART. 617-QUINQUIES OF THE PENAL CODE)

This offence is committed by anyone who, save in cases permitted by law, in order to intercept communications related to a computer or electronic telecommunications system or between two systems, or to block or disrupt such communications, procures, holds, produces, reproduces, disseminates, imports, communicates, delivers, or otherwise makes available to others, or installs equipment, programs, codes, passwords or other means capable of intercepting, blocking or disrupting communications related to a computer or electronic telecommunications system or between multiple systems.

The mere installation of the equipment is unlawful, therefore, regardless of whether it is actually used. Hence, it is not necessary to prove that interception, blocking or disruption of

communication has occurred; it is sufficient to objectively establish the potentially harmful nature of the equipment.

EXTORTION (Article 629 of the Penal Code)

Among the notable innovations introduced by the Italian Cybersecurity Law is the new offence of 'Cyber Extortion', inserted into the third paragraph of Article 629, which reads as follows:

'Anyone who, with violent acts or threats, compels someone to do or omit something, thereby obtaining an illegitimate gain for themselves or others and causing detriment to others, shall be punished by a term of imprisonment ranging from five to ten years and a fine between EUR 1,000 and EUR 4,000.

The punishment shall be a term of imprisonment from seven to twenty years and a fine of between EUR 5,000 and EUR 15,000, if any of the circumstances mentioned (in the last paragraph of the preceding article) or in the third paragraph of Article 628 apply.

Anyone who - through the conduct referred to in Articles 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater, and 635-quinquies, or by threatening to carry out such conduct - compels someone to do or omit something, thereby procuring an illegitimate gain for themselves or others and causing detriment to others, shall be punished by a term of imprisonment ranging from six to twelve years and by a fine of between EUR 5,000 and EUR 10,000. The punishment shall be a term of imprisonment ranging from eight to twenty-two years and a fine of between EUR 6,000 and EUR 18,000, if any of the circumstances mentioned in the third paragraph of Article 628 apply, and also in cases where the act is committed against a person without capacity due to age or infirmity'.

With this new provision, the legislature saw fit to legislate for an independent offence for so-called ransomware attacks, i.e. conduct aimed at unlawfully encrypting third-party data and demanding payment in return for decryption: this could involve, for example, the disclosure of sensitive information about a company's employees or its customers, or confidential data that, if disclosed, could harm the reputation of an individual or a company.

The new offence of cyber extortion has been inserted into Article 24-bis of the Decree and could lead to the entity on whose behalf the offence is committed being held liable, and to the

application of a monetary penalty ranging from 300 to 800 units, and to the disqualification penalties provided for in Article 9, paragraph II, for a duration of not less than two years.

The offence of cyber extortion may occur in cases where the aim is to give the entity a competitive advantage, for example, when the conduct seeks to unlawfully access a competitor's computer system.

DAMAGING COMPUTER INFORMATION, DATA AND IT PROGRAMS (ARTICLE 635-BIS OF THE PENAL CODE)

This offence is committed when an individual '*destroys, degrades, erases, alters or suppresses computer information, data or programs belonging to others'.*

The penalty is increased:

1) if the act is committed by a public official or public service officer, by abusing their powers or violating the duties inherent in their function or service, or by someone who works lawfully or unlawfully as a private investigator, or by abusing their role as a system operator;

2) if the perpetrator uses threats or violence to commit the act, or is visibly armed.

The offence is committed, for example, if an individual erases data from a computer's memory drive without prior authorisation from the computer's owner.

DAMAGING COMPUTER OR ELECTRONIC TELECOMMUNICATIONS SYSTEMS (ART. 635-QUATER OF THE PENAL CODE)

This offence is committed when an individual '*through the conduct referred to in Article 635-bis (damage to data, information, and computer programs), or by introducing or transmitting data, information or programs, destroys, damages, or renders unusable (in whole or in part) the computer or electronic telecommunications systems of others, or seriously obstructs their functioning'*.

The penalty is increased:

1) if the act is committed by a public official or public service officer, by abusing their powers or violating the duties inherent in their function or service, or by anyone who works lawfully or unlawfully as a private investigator, or by abusing their role as a system operator;

2) if the perpetrator uses threats or violence to commit the act, or is visibly armed.

Note that if the alteration of data, information, or programs renders the system unusable or seriously obstructs its functioning, the offence of damage to computer systems will be established, rather than the offence of damage to data under Article 635-bis of the Penal Code.

The offence is established in cases of damage to or deletion of data or programs contained in the system, carried out directly or indirectly (for example, by inserting a virus into the system).

UNAUTHORISED POSSESSION, DISSEMINATION AND INSTALLATION OF COMPUTER EQUIPMENT, DEVICES OR PROGRAMS FOR THE PURPOSE OF DAMAGING OR DISRUPTING A COMPUTER OR ELECTRONIC TELECOMMUNICATIONS SYSTEM (ART. 635-QUATER.1 OF THE PENAL CODE)

Anyone who - with the aim of unlawfully damaging a computer or electronic telecommunications system, or the information, data, or programs contained therein or related to it, or to cause the total or partial disruption or alteration of its functioning - unlawfully procures, possesses, produces, reproduces, imports, disseminates, communicates, delivers, or otherwise makes available to others or installs computer equipment, devices, or programs, shall be punished by a term of imprisonment up to two years and by a fine of up to EUR 10,329.

The term of imprisonment will be from two to six years if any of the circumstances referred to in Article 615-ter(2) no. 1, apply.

The term of imprisonment is further increased from three to eight years if the offence involves the computer or electronic telecommunications systems referred to in Article 615-ter(3).

COMPUTER FRAUD (ART. 640-TER OF THE PENAL CODE)

Article 640-ter, para. 1, of the Penal Code states that '*anyone who - by altering in any way the functioning of a computer or electronic telecommunications system or by unlawfully manipulating the data, information or programs contained in or related to a computer or*

electronic telecommunications system - procures an illegitimate gain for themselves or others, thereby causing detriment to others, shall be punished by a term of imprisonment ranging from six months to three years and by a fine of between 100,000 and 2,000,000 lire'.

The criminal conduct, therefore, consists of altering the functioning of a computer system or unlawfully handling data, information, or programs contained in a computer system.

Computer fraud is relevant, under the Decree, if committed against the State or another public entity. This offence is committed where a person - by altering the operation of a computer or electronic communications system or manipulating the data contained therein - obtains an illegitimate benefit to the detriment of the State or other public body. The offence may also involve the alteration of PA computer records in order to falsely indicate essential conditions for participation in tenders (e.g. registration in professional registers or rolls) or in order to subsequently produce documents that attest to non-existent facts or circumstances, or to modify tax/social security data concerning the company (e.g. Model 770) that have already been send to the PA. The offence may also be committed if, after obtaining funding, the PA's computer system is breached in order to insert an amount higher than that legitimately obtained.

COMPUTER FRAUD BY PERSONS PROVIDING ELECTRONIC SIGNATURE CERTIFICATION SERVICES (ART. 640-QUINQUIES OF THE PENAL CODE)

This provision punishes individuals who, in the exercise of their electronic signature certification services, in order to obtain an illegitimate benefit for oneself or others or to cause detriment to others, violate legal obligations governing the issuance of a qualified signature certification.

Article 640-quinquies of the Penal Code is justified by the increasing prevalence of electronic signature systems and, consequently, by the legislature's wish to identify a specific type of computer fraud related to the unlawful conduct of electronic signature certifiers, who, based on the certifying authority expressly granted to them by law, are deemed to be public officials.

The violation of legal obligations by the certifier is criminally relevant only if the offence was committed in order to obtain an illegitimate benefit for oneself or for others, or to cause detriment to others.

E.1.3. Copyright infringement offences

Article 25-novies, on '*copyright infringement offences'*, was introduced by Law 99/2009 and amended by Law 93/2023.

It extended the administrative liability of entities to offences under Law 633/1941 on the protection of copyright and other rights associated with its exercise (the '*Copyright Law'*, below).

Law 93/2023, entitled '*Provisions for the prevention and prosecution of the unlawful dissemination of copyright-protected content through electronic communication networks',* aimed at combating online piracy, strengthened the protection of intellectual property and copyright and expanded the catalogue of predicate offences triggering the administrative liability of entities under the Decree.

Below is a description of the offences punishable under Article 25-novies of the Decree, which following a risk analysis were considered theoretically relevant for GIMA.

DISCLOSURE OF A COPYRIGHT-PROTECTED WORK ON ELECTRONIC TELECOMMUNICATIONS NETWORKS (ARTICLE 171, PARA. 1 A-BIS AND PARA. 3 OF THE ITALIAN COPYRIGHT LAW)

In relation to the criminal offence under Article 171 of the Italian Copyright Law, the Decree considered only two scenarios:

1. (i) where a copyright-protected work or part thereof is made available to the public, by insertion into a telecommunications network with connections of any kind;
2. (ii) where a copyright-protected work not intended for publication is made available to the public, by insertion into a telecommunications network with connections of any kind, or where the authorship of the work is usurped or the work is distorted, mutilated or otherwise altered, where this adversely affects the author's reputation or good name.

In the first scenario, the legal interest protected is the economic interest of the author, whose expectations of profit may be harmed by the free circulation of their work online. In the second scenario, the legal interest protected is not the rights holder's expectation of economic earnings but their honour and reputation.

This offence could, for example, be committed in the interest of the Company if copyrighted content were uploaded to the corporate network for use in the course of business activities.

DUPLICATION OF COMPUTER PROGRAMS FOR PROFIT, OR IMPORT, DISTRIBUTION, SALE, POSSESSION FOR COMMERCIAL PURPOSES OF PROGRAMS CONTAINED IN MEDIA NOT MARKED BY THE ITALIAN COPYRIGHT AUTHORITY (SIAE) (ART. 171-BIS OF THE ITALIAN COPYRIGHT LAW)

This provision aims to protect the proper use of software and databases.

In relation to software, this provision criminalises the unauthorised duplication, as well as the importation, distribution, sale, possession for commercial or business purposes, and rental of 'pirated' programs.

The offence is committed by anyone who unlawfully duplicates computer programs for profit or, for the same purposes, imports, distributes, sells, holds for commercial or business purposes or leases computer programs on media not marked by the Italian Society of Authors and Publishers (SIAE - Copyright Authority).

The conduct is also punishable if it involves any means solely intended to permit or facilitate the unauthorised removal or circumvention of program protection devices.

The second paragraph of the same provision also punishes anyone who, for profit, using media not marked by the SIAE (Italian Copyright Authority), reproduces, transfers to another medium, distributes, communicates, presents or demonstrates in public the content of a database or performs extraction or re-utilisation of the database in violation of the Italian Copyright Law.

The offence requires only a subjective intention to achieve an economic gain; therefore, any conduct beyond purely financial gain (e.g. to obtain a profit through goods or services) is also caught by the provision and is therefore criminally relevant.

This offence could, for example, be committed in the interest of the Company if non-original software were used for working purposes, in order to save on the cost of licensing original software.

CAPITOLO E.2

E.2.1 Sensitive processes in the context of computer offences and copyright infringement offences

Although it may seem unlikely, at first glance, for cybercrimes to occur in companies operating in sectors far removed from the tech/cyber industry, such a possibility is no longer so remote in a context in which criminal actions, carried out using digital tools, serve as the 'means' to commit other types of offences, the risk of which is statistically more like in production environments.

Consider, for example, a hypothetical case involving a newly hired sales manager of the company Alpha S.p.A., a former employee of Beta S.r.l., who - despite having their access privileges revoked - manages to unlawfully access Beta S.r.l.'s computer systems and extract confidential personal data and commercial information to exploit it for the benefit of Alpha S.p.A. In this case, it could be argued that the computer crime of '*Unauthorised access to a computer or electronic communications system'* (Art. 615-ter of the Penal Code and Art. 24-bis of Legislative Decree 231/2001) is committed concurrently with one of the offences against industry and commerce pursuant to Art. 25-bis.1 of the said Decree.

Another hypothetical case to consider: an employee of Gamma S.r.l. suffers a serious injury while using machinery lacking a 'protective guard', and the incident is recorded by the facility's surveillance camera system. Before calling the emergency services, the facility manager tampers with the surveillance system's storage device, deleting the recordings of the incident, and then installs the protective guard on the machinery. The conduct described could be caught by Art. 635-quater of the Penal Code, '*damaging computer or electronic telecommunications systems'*, as provided and punishable under Art. 24-bis of the Decree, as it was committed in the interest and for the benefit of Gamma S.r.l., and sought to avoid penalties for health and safety violations and also for potential reputational damage.

That said, following an in-depth analysis of the company's operations, the following are the main Sensitive Processes that the Company has identified within its organisation:

1) use, management, and monitoring of corporate IT systems;

2) use of company devices;

3) management of software licenses;

4) use of databases;

5) management of servers or websites;

6) management of marketing and advertising activities.

CHAPTER E.3

General principles of conduct

The aim of this Special Part is to ensure that employees, governing bodies and peripheral operators (consultants, service providers, etc.), to the extent they may be involved in Sensitive Processes, adhere to rules of conduct in line with the provisions of this Special Part, in order to prevent and deter computer offences and copyright infringement offences.

In carrying out company activities, and particularly in Sensitive Processes, it is expressly forbidden for the aforementioned individuals, regardless of their relationship with the Company, to engage or collaborate in or cause conduct, acts or omissions that, individually or together, directly or indirectly, trigger the offences covered in this Special Part (Arts. 24-bis and 25-novies of the Decree).

Specifically, the following are forbidden:

- engaging in conduct that (i) triggers an offence under the Decree or (ii), although not triggering an offence *per se*, could prepare for the commission of an offence (e.g. lack of oversight);
- disclosing information about corporate IT systems that could reveal vulnerabilities and/or unauthorised or improper uses;
- using the Company's IT systems for purposes unrelated to the assigned role;
- exploiting vulnerabilities or inadequacies in the security measures of clients' or third party computer or electronic telecommunications systems, in order to gain access to resources or information beyond what one is permitted, even if such intrusion does not cause damage to data, programs, or systems;
- tampering with, removing or destroying company or third-party IT assets, including digital archives, data, and programs;
- independently installing unauthorised software on company-provided PCs;
- illegally using material protected by copyright.

In carrying out their respective activities/functions, in addition to the rules set out in the Model and this Special Part, Recipients are required to know and comply with all company rules on:

- management of logical access to networks, systems, data, and applications;
- management of personal credentials (username and password);
- proper handling of information obtained for operational reasons.

To mitigate the risk of commission of computer offences and copyright infringement offences and, consequently, also to ensure compliance with applicable regulatory provisions, the Company fulfils the following obligations in connection with its corporate operations:

1. it provides Recipients with adequate information on the proper use of corporate IT tools and access credentials for accessing the main IT subsystems used in the Company;
2. it restricts, using differentiated access authorisations, the use of IT systems and access thereto by Recipients, exclusively for purposes related to their assigned job duties;
3. it conducts, where possible, periodic checks on the corporate IT network, in compliance with privacy laws, existing collective bargaining agreements and with the Workers' Statute, in order to identify anomalies;
4. it implements and maintains adequate physical defences to protect the Company's servers;
5. it implements and maintains adequate physical and logical defences to protect other corporate IT systems;
6. it conducts periodic inventories of software and databases in use within the company and verifies that their use is authorised by appropriate licenses;
7. it conducts, where possible, checks on the content of the corporate website.

CAPITOLO E.4

Specific procedural principles

To implement the rules and comply with the prohibitions listed in the previous Chapter, the principles described below must be adhered to, in addition to the General Rules and Principles already outlined in the General Part of this Model.

In particular, the Company ensures compliance with the following rules.

1) Use, management, and monitoring of corporate IT systems

2) Use of company devices

a) it is forbidden to introduce and connect computers, peripherals, other equipment or software to the corporate IT system without prior authorisation from the person in charge of the IT area;

b) it is forbidden to modify the configuration of fixed or mobile workstations without the consent of the responsible party;

c) it is forbidden to obtain, possess or use software and/or hardware tools that could be used to compromise the security of computer or electronic telecommunications systems (e.g. password-cracking tools, vulnerability scanners, decryption tools, traffic interception tools, etc.);

d) it is forbidden to obtain access credentials to access computer or electronic telecommunications systems belonging to the Company or to clients or third-parties using methods not authorised by the Company;

e) it is forbidden to disclose, transfer or share with internal or external personnel (or otherwise make accessible to third parties) one's access credentials to enable access to corporate, client or third-party systems and networks;

f) it is forbidden to access another's IT system (including a colleague's) without express authorisation;

g) it is forbidden to tamper with, remove or destroy corporate, client, or third-party IT assets, including digital archives, data, and programs;

h) it is forbidden to attempt to compromise the security controls of client or third-party computer or electronic telecommunications systems, unless this is specifically required and authorised by special contractual agreements or falls within one's job duties;

i) it is forbidden to exploit vulnerabilities or deficiencies in the security measures of clients' or third-parties' computer or electronic telecommunications systems, in order to gain access to resources or information beyond what is permitted, even if such intrusion does not cause damage to data, programs, or systems;

j) it is forbidden to share information system controls and usage with unauthorised persons inside or outside the Company;

k) it is forbidden to distort, obscure or substitute one's identity, and it is forbidden to send emails containing false information or concealing viruses or other programs capable of damaging or intercepting data;

l) the Company:

1. requires employees and other authorised individuals to sign a special commitment undertaking the proper use of corporate IT resources;
2. provides periodic training to employees on relevant topics in order to raise awareness of the risks associated with improper use of corporate IT resources;
3. alerts employees not to use company devices for personal purposes or for purposes unrelated to their work;
4. informs employees and other authorised individuals of the requirement not to leave one's own IT systems unattended, and to lock them with their access codes when leaving their workstations;
5. configures IT systems to automatically lock after a period of inactivity;
6. provides external internet (incoming and outgoing) access exclusively to the IT systems of employees or third parties who require such access for work-related or administrative reasons;
7. restricts access to server rooms to authorised personnel only;
8. protects, as far as possible, every corporate IT system against the unauthorised installation of hardware devices capable of intercepting communications related to a computer or electronic telecommunications system or between multiple systems, or capable of blocking or disrupting them;
9. deletes accounts, particularly those assigned to system administrators, upon termination of the relevant contractual relationship;
10. promptly informs IT system managers of the commencement and end of employment or collaboration relationships, to facilitate initiating the process of granting, modifying, or revoking access permissions;
11. equips every IT system with adequate firewalls and antivirus software and ensures, where possible, that these cannot be deactivated;
12. prevents the installation and use of software not approved by the Company and unrelated to the professional activities performed on its behalf;

13. restricts access to programs and websites that may serve as vehicles for the distribution and dissemination of viruses capable of damaging or destroying IT systems or the data contained therein;

14. if wireless connections are used for internet access, protects them by setting an access key to prevent unauthorised external parties from illicitly accessing the Company's Internet network, via its routers, and committing offences attributable to employees;

15. implements an authentication process using usernames and passwords, assigning a limited system resource management profile specific to each employee, intern or other authorised user of the corporate IT systems;

16. adequately informs employees and other authorised individuals of the importance of keeping their access codes (username and password) confidential;

17. restricts external access to the corporate IT network, by adopting and maintaining authentication systems different from or additional to those used for internal access by employees and other authorised individuals.

3) Management of Software Licenses

a) The Company ensures:

i. that a register of all third-party software used for corporate activities is created and maintained, including tracking of the terms of use of their respective licenses;
ii. periodic checks on software installed on company PCs, in order to identify installations of unauthorised programs, including the enforced deletion of any unauthorised content;
iii. periodic training/information sessions for employees on relevant topics.

***4)* Management of marketing and advertising activities**

a) In the context of these activities, the Company:

i. informs Recipients of the importance of proper use of copyright-protected material, particularly regarding the correct selection and use of images in advertising materials;
ii. conducts systematic and formalised checks, to the extent of its competence, on the source of images used for presentations and/or advertising materials;
iii. ensures that the necessary exploitation rights are obtained from the rights holder before third-party copyright-protected works can be used for promotional purposes;

iv. ensures that clauses are included in contracts with communication companies or advertising agencies that require compliance with copyright protection laws, in addition to the Model 231 Clauses.

b) the Company identifies the individuals involved in the decision-making process for altering the corporate website and controlling content uploaded to the website and to the Company's social media accounts;

c) the Company ensures that copyright-protected works can be used on the website (or equivalent channels, e.g. social media) or on billboards and newspaper advertisements only after the necessary exploitation rights have been obtained from the rights holder;

d) the Company has an established authorisation process for published material, following a prior content review by the competent functions;

e) the Company periodically checks the use of non-authorised material;

f) the Company verifies the legitimate use of copyright-protected works not only in its external marketing and promotional activities but also in the dissemination of material within the Company.

Chapter E.5

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the scope of their respective duties and responsibilities, comply with the rules and principles set out in this Special Part.

In particular, the SB has the following duties:

- to monitor the effectiveness of the procedural principles set out therein, and of the corporate rules adopted to prevent the offences outlined in this Special Part;
- to propose any necessary changes to Sensitive Processes attributable to potential changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The OdV must be promptly informed in the event of violation of the specific procedural principles contained in this Special Part or of the corporate procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART - F -

Environmental offences

CHAPTER F.1

Environmental offences (Art. 25-undecies of Legislative Decree 231/2001)

This Special Part deals with environmental offences, referenced in Art. 25-undecies of the Decree.

Italian Legislative Decree 121/2011 extended the administrative liability of companies and entities to a series of environmental offenses. Subsequently, Law 68/2015 introduced Title VI-bis - '*Offenses against the environment'* - into Book II of the Penal Code amending and supplementing Article 25-undecies of the Decree by including additional environmental offenses which, if committed, trigger administrative liability under the Decree.

Below is a brief description of the offences covered in this Part that are listed in Art. 25-undecies of the Decree ('Environmental Offences', below), which may be potentially relevant in the context of the Company's operations.

F.1.2 Offences under Legislative Decree 152/2006 (Environmental Code)

UNAUTHORISED WASTE MANAGEMENT ACTIVITIES (ART. 256 OF THE ENVIRONMENTAL CODE)

Article 256 is the most important provision in the disciplinary and sanctions system for waste management, as it regulates a multitude of waste management-related activities (i.e. waste collection, transport, recovery, disposal, trade, and intermediation), for both hazardous and non-hazardous waste.

Regarding the subjective element of the conduct (*mens rea*), since the offence is in the nature of a 'misdemeanour' (*contravvenzione*), this means that the offences under the first paragraph of this article are punishable whether committed with negligence or premeditated intent.

One should emphasise the strict approach taken by the courts when interpreting and applying this rule. Even if a company is authorised to recover waste, it can still be held liable for complicity if it receives waste from an unauthorised intermediary or carrier, since the recipient is obliged to verify that all parties providing waste for treatment have the necessary authorisation.

VIOLATION OF OBLIGATIONS OF NOTIFICATION AND KEEPING OF MANDATORY REGISTERS AND FORMS (ART. 258 OF THE ENVIRONMENTAL CODE)

Article 258 stipulates that companies collecting and transporting their own non-hazardous waste shall be punished if they fail to voluntarily adhere to the waste traceability control system (SISTRI) and transport waste without the mandatory forms under Art. 193, or if they provide incomplete or inaccurate information in the forms.

Additionally, the rules on false statements (*falsità ideologica*) by a private individual in an official document are extended to cases where a waste analysis certificate is drawn up

containing false information about the nature, composition and chemical/physical characteristics of waste, or where use is made of a false certificate during transport.

Liability also arises where the information referenced in paras. 1 and 2 is formally incomplete or inaccurate, but data inserted in the communication to the National Waste Registry, in the waste loading/unloading registers, in the waste identification forms for transported waste and in other mandatory accounting records enable the necessary information to be reconstructed. Similarly, liability arises where the information under para. 4 is formally incomplete or inaccurate but contains all the specifics necessary to reconstruct the information that is legally required, and also if there is a failure to send the required information to the relevant authorities.

ILLEGAL TRAFFICKING OF WASTE (ARTICLE 259, ENVIRONMENTAL CODE)

The offences of illegal waste trafficking under Art. 259(1) refer exclusively to cross-border shipments of waste. This article, since it refers to Regulation (EC) 259/93 for the definition of illegal trafficking, must be considered as a blank criminal law provision.

The second paragraph stipulates that, in the event of a conviction, the confiscation of the means of transport is mandatory.

WASTE TRACEABILITY ELECTRONIC CONTROL SYSTEM (SISTRI) (ART. 260-BIS OF THE ENVIRONMENTAL CODE)

Art. 260-bis punishes the falsification, omission or fraudulent alteration of documentation enabling waste traceability, extending here too the rules on false statements (*falsità ideologica*) by a private individual in an official document.

F.1.3 Offences under Book II, Title VI-bis, of the Penal Code

ENVIRONMENTAL POLLUTION (ART. 452-BIS OF THE PENAL CODE)

This provision punishes anyone who unlawfully causes significant and measurable harm or deterioration to waters, air, soil, subsoil, an ecosystem, or biodiversity.

The penalty is increased by one-third to one-half if the pollution occurs in a protected natural area or an area subject to landscape, environmental, historical, artistic, architectural, or

archaeological constraints, or if it harms protected animal or plant species. Furthermore, the penalty is increased by one-third to two-thirds if the pollution causes deterioration, harm or destruction of a habitat within a protected natural area or an area subject to such constraints. These aggravating circumstances were introduced into Art. 452-bis of the Penal Code by **Law 137/2023**, which converted Decree-Law no. 105 of 10 August 2023 (the so-called 'Justice Decree').

UNPREMEDITATED OFFENCES AGAINST THE ENVIRONMENT (ART. 452-QUINQUIES OF THE PENAL CODE)

This provision provides that if any of the acts referred to in Arts. 452-bis and 452-quater are committed negligently; the penalties provided for therein shall be reduced by one-third to two-thirds. The penalties are further reduced if the acts in question result in a risk of environmental pollution or environmental disaster.

ORGANISED ACTIVITIES FOR THE ILLEGAL TRAFFICKING OF WASTE (ART. 452-QUATERDECIES OF THE PENAL CODE)

For this offence to be committed, at least two operations is required: the preparation of organised means and ongoing organised activities, the act of transferring, receiving, transporting, exporting, importing or otherwise managing waste, the large quantity of waste, and the unlawful nature of the waste management activity.

This offence is (i) necessarily habitual, as its commission requires the repetition of similar acts/conduct; (ii) an offence of 'pure conduct', as the criminal culpability in question is focused on the conduct itself; and (iii) characterised by specific intent to pursue an illegitimate gain or profit.

The offence was introduced by Legislative Decree 21/2018 and replaces Art. 260 of Legislative Decree No. 152/2006, which was repealed by the aforementioned Decree. As specified in Art. 8 of Legislative Decree 21/2018, '*from the date of entry into force of this Decree, any references to the provisions repealed by Art. 7, wherever they appear, shall be understood as referring to the corresponding provisions of the Penal Code'*.

CHAPTER F.2

Sensitive Processes in the context of corporate offences

The Sensitive Processes identified by the Company in relation to environmental offences are as follows:

- waste management and disposal;
- selection and management of environmentally conscious suppliers;
- environmental compliance management (management of mandatory environmental obligations and declarations required by law).

CHAPTER F.3

General Principles of Conduct

The aim of this Special Part is to ensure that all Recipients adopt rules of conduct in compliance with its provisions, in order to prevent the occurrence of the offences considered therein.

All activities that present a potential risk profile in connection with environmental offences must be carried out in conformity with the laws in force, with the values and policies of the Company and the rules contained in this Model and in the documents referred to. In particular, the company's policy regarding the mitigation of risks related to the commission of environmental offences is guided by the following principles:

- promotion of a sense of environmental responsibility among all Recipients;
- general assessment of the potential impacts of the Company's activities on the local environment;
- reduced production of waste products;
- cooperation with the relevant public authorities;
- encouraging suppliers to respect environmental standards;
- compliance with applicable laws and regulations.

Furthermore, the Company:

- ensures that the requirements of laws and regulations applicable to environmental protection are identified and correctly applied;

- raises awareness among all individuals operating within the Company, at various levels, by organising suitable information activities and training programs;
- where the Company, for the purpose of its activities, is the recipient of an environmental authorisation or concession, all Recipients must strictly adhere to the conditions and parameters specified therein.

CHAPTER F.4

Specific procedural principles

When engaged in the Sensitive Processes identified in this Special Part, the Company – also by adopting specific procedures – ensures that the following general principles and rules are respected.

1) Waste Management

a. The Company, particularly in relation to the management of waste produced, oversees the proper management of such waste, also where entrusted to third parties, and reports any irregularities to the relevant departments. Specifically:

i. the Company entrusts waste collection, transport, recovery and disposal activities exclusively to authorised firms, in compliance with company procedures;
ii. when assigning waste disposal or recovery activities to authorised companies, the Company verifies: (a) the validity date of the authorisation; (b) the type and quantity of waste for which the waste disposal/recovery authorisation has been issued; (c) the location of the disposal facility; and (d) the treatment or recovery method;
iii. while waste transport activities are being carried out, the Company verifies: (a) the validity date of the authorisation; (b) the type and registration number of the vehicle; (c) the authorised EWC (European Waste Catalogue) codes;
iv. it conducts periodic checks on the enterprises to which these activities are entrusted;
v. in contracts with these companies, the Company will ensure the inclusion of clauses (in addition to the mandatory Model 231) to protect the Company, requiring suppliers/contractors/subcontractors to guarantee that they hold all the necessary authorisations to perform the activities covered by the contract, and also provides for the obligation to promptly notify the Company if the authorisations received have been amended or revoked, etc.

CHAPTER F.5

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the scope of their respective duties and responsibilities, comply with the rules and principles set out in this Special Part.

In particular, the SB has the following duties:

- to monitor the effectiveness of the procedural principles provided therein, or the principles contained in company policies adopted for the prevention of offences outlined in this Special Part;
- to propose any necessary changes or additions of the Sensitive Process identified in this Special Part, in light of any changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The SB must be promptly informed of any infringements of the specific procedural principles contained in this Special Part, or of any infringements of company procedures, policies and standards related to the Sensitive Process identified above and to the prevention of environmental offences.

The SB also has authority to access, or to request its delegatees to access, any and all documentation if pertinent to the performance of its duties.

SPECIAL PART – G –

Offences related to trademarks and distinguishing marks and offences against industry and commerce

CHAPTER G.1

G.1.1. Offences related to trademarks and distinguishing marks

The offences of '*Falsification, alteration or use of trademarks or distinguishing marks or patents, models and designs'* and '*Bringing into the State and selling products bearing false*

signs', as provided for in Articles 473 and 474 of the Penal Code, respectively, and referred to in Art. 25-bis of the Decree, unlike the offences described below (falling under "*Offences against industry and commerce*"), fall within the category of '*Offences against the public trust'*.

These offences aim to protect the public's trust in the authenticity and veracity of the distinguishing marks of industrial products (trademarks) or of copyright-protected works (patents, industrial models, and industrial designs).

Below is a brief description of the offences under Articles 473 and 474 of the Penal Code, as they are considered relevant in theory to the Company's activities.

FALSIFICATION, ALTERATION OR USE OF TRADEMARKS OR DISTINGUISHING MARKS OR OF PATENTS, MODELS AND DESIGNS (ART. 473 OF THE PENAL CODE)

Article 473 of the Penal Code punishes:

- anyone who, being aware of the existence of the industrial property right, falsifies or alters national or foreign trademarks or distinguishing marks of industrial products;
- anyone who, without having committed falsification or alteration, uses such falsified or altered trademarks or signs.

The provision aims to protect distinguishing marks or industrial products, namely:

- *trademarks*: signs (emblems, figures, names, etc.) intended to distinguish goods or products of a specific company;
- *patents*: certificates granting the exclusive right to use an invention or discovery;
- *industrial designs*: figurative representations of any industrial good or product;

- *industrial models:* archetypes of a discovery or a new industrial application (e.g. ornamental models and utility models).

The criminal conduct consists of falsifying the distinguishing mark in such a way as to create confusion in distinguishing the signs, and may thus involve:

- *falsification,* i.e. creating something entirely similar to a different thing, so as to misrepresent its true nature;

- *alteration*: changing the appearance, substance or nature of a thing.

BRINGING INTO THE STATE AND SELLING PRODUCTS BEARING FALSE SIGNS (ART. 474 OF THE PENAL CODE)

The offence is committed when, outside the cases of complicity in the offences provided for in Article 473 of the Penal Code, industrial products with falsified or altered trademarks or other distinguishing marks, whether national or foreign, are introduced into the territory of the State in order to make a profit.
Anyone who holds for sale, offers for sale or otherwise distributes falsified or altered products for the purpose of making a profit is also punishable under this provision.

These offences are punishable on condition that applicable laws, EU regulations and international conventions on the protection of intellectual or industrial property have been respected.

G.1.2. Offences of disruption of industrial or commercial freedom

Law 99/2009, containing '*Provisions for the development and internationalisation of enterprises, and provisions on energy'*, introduced (by Art. 15, para. VII) into Legislative Decree 231/2001 Article 25-bis.1 '*Offences against industry and commerce'*.

DISRUPTING INDUSTRIAL OR COMMERCIAL FREEDOM (ART 513 OF THE PENAL CODE)

This offence is committed by anyone who uses violence against property or fraudulent means to prevent or disrupt the operation of an industry or business.

The offense is committed in the following ways:

- use of violence against property, which occurs whenever property is transformed, damaged or when its designated use is altered;
- use of fraudulent means (acts of unfair competition under Art. 2598 of the Italian Civil Code):

1. misleading advertising;
2. defamatory advertising;
3. use of registered trademarks belonging to others;
4. poaching of employees;
5. parasitic competition.

UNLAWFUL COMPETITION USING THREATS OR VIOLENCE (ART. 513-BIS OF THE PENAL CODE)

This offence is committed when, in the course of commercial, industrial or productive activities, acts of competition are carried out with violence or intimidation.

Unfair competition is a well-known problematic. For the purposes of the criminal law, however, one must act with intimidation or violence with a view to controlling or, at least, influencing commercial, industrial or productive operations, thereby undermining the market principle aimed at ensuring free competition; thus, any form of violence or threat that results in a competitor being intimidated, for example during a tendering procedure, could be caught by this criminal offence.

FRAUD AGAINST NATIONAL INDUSTRIES (ART. 514 OF THE PENAL CODE)

Fraud against national industries is committed whenever domestic industry is harmed by the act of offering for sale or otherwise putting into circulation (on domestic or foreign markets) industrial products bearing names, trademarks or distinguishing marks that have been falsified or altered.

FRAUDULENT TRADING (ART. 515 OF THE PENAL CODE)

This offence is committed when, in the course of commercial activities or in a retail establishment open to the public, a movable asset is delivered to a purchaser that is different from the one agreed upon, or differs in origin, provenance, quality, or quantity from what was declared or agreed.

SALE OF NON-GENUINE FOODSTUFFS AS GENUINE (ART. 516 OF THE PENAL CODE)

This offence is committed by anyone who offers for sale or otherwise markets non-genuine foodstuffs as genuine.

SALE OF INDUSTRIAL PRODUCTS WITH MISLEADING MARKS OR SIGNS (ART. 517 OF THE PENAL CODE)

This offence punishes any person who holds for sale, offers for sale or otherwise distributes copyright-protected works or industrial products bearing names, trademarks or distinguishing marks, national or foreign, that are likely to mislead the buyer as to the origin, provenance or quality of the work or product.

MANUFACTURE AND SALE OF GOODS MADE BY USURPING INDUSTRIAL PROPERTY RIGHTS (ART. 517-TER OF THE PENAL CODE)

Without prejudice to the application of Art. 473 of the Penal Code (falsification, alteration or use of trademarks or distinguishing marks or patents, models and designs) and Art. 474 of the Penal Code (bringing into the State and selling products bearing false signs), this provision punishes anyone who, being in a position to know of the existence of the industrial property right, manufactures or applies industrial processes to objects or to other goods produced in violation of or usurping an industrial property right. The provision also penalises anyone who, for profit, introduces such goods into the territory of the State, holds them for sale, offers them for sale directly to consumers or puts them into circulation.

The above-mentioned offences are punishable provided that applicable domestic laws, EU regulations and international agreements on the protection of intellectual or industrial property have been observed.

CHAPTER G.2

Sensitive Processes

The following are the main Sensitive Processes identified by the Company in relation to the offences covered in this Special Part, which the Company has identified within its organisation:

- management of IT systems, particularly the purchase and management of software licenses;

- management of website content;
- management of marketing and advertising activities and preparation of promotional/advertising materials;
- management of sales.

CHAPTER G.3

General Principles of Conduct

In carrying out Sensitive Processes, Recipients shall in general be familiar with and observe:

- the rules of fair and lawful competition;
- the system of company procedures and safeguards in place for the control and monitoring of products and raw materials purchased from third parties and intended for processing;
- the generally applicable Italian legislation in this area.

It is strictly forbidden to engage in, collaborate in or cause acts or conduct which, individually or together, directly or indirectly, trigger the offences outlined above (Arts. 25-bis and 25-bis.1 of the Decree).

In the context of the aforementioned conduct it is forbidden, in particular:

a) to use names or distinguishing marks in the marketing of products that are likely to cause confusion with names or distinguishing marks belonging to or legitimately used by other companies;
b) to use patents, models, or industrial designs belonging to others without having first obtained a license;
c) to provide a description of a product (including its composition) that does not exactly match its actual characteristics;
d) to indicate a product origin that does not exactly correspond to its place of production, in violation of applicable legislation;
e) to introduce into the Italian State products with false indications of origin;
f) to introduce into the Italian State products with false distinguishing marks;

g) to disseminate information and/or opinions about a competitor's products and activities that could potentially discredit it;

h) to fail to comply strictly with the rules of commercial fairness established by the Company, and with applicable legislative and regulatory provisions protecting the market, consumers and end customers in general, in compliance with the principles of transparency, good faith, and full information provision;

i) to engage in acts of competition involving violence or intimidation during a commercial activity.

CHAPTER G.4

G.4.1. Specific procedural principles

In order to implement the rules listed in the previous Chapter, the principles set out below must be adhered to, as well as the general principles contained in the General Part of this Model.

- not to offer for sale or distribute copyright-protected works or industrial products bearing names, trademarks, or distinguishing marks, national or foreign, that are likely to mislead the buyer as to the origin, provenance, or quality of the work or product;
- to include clauses, in contracts with suppliers, guaranteeing that they will not infringe third party rights in the course of their activities.

CHAPTER G.5

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the limits of their respective duties and responsibilities, properly observe the rules and principles enshrined in this Special Part and in the company procedures to which that Part explicitly or implicitly refers.

In particular, the SB has the following duties:

- to monitor the effectiveness of the principles contained in company policies adopted for the prevention of offences outlined in this Special Part;

- to propose any necessary changes to Sensitive Processes attributable to potential changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The SB shall be promptly informed of any infringements of the specific procedural principles contained in this Special Part, or of infringements of the company procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART – H –

Recruitment of undocumented third country nationals and unlawful intermediation and exploitation of labour

CHAPTER H.1

H.1.1. Recruitment of undocumented third country nationals (Article 25-duodecies of Legislative Decree 231/2001)

This Special Part refers to the '*recruitment of undocumented third country nationals'*, introduced as a predicate offence into the Decree (Art. 25-duodecies) by Legislative Decree 109/2012, implementing Directive 2009/52/EC.

This offence is committed when an employer hires foreign workers who do not possess a valid residence permit, or whose permits have expired and an application for renewal has not been

submitted by the legally prescribed deadline, or whose permits have been revoked or annulled, provided that the workers recruited are:

a. more than three in number;
b. minors below the legal working age;
c. subject to other particularly exploitative working conditions as indicated in the third paragraph of Art. 603-bis of the Penal Code.

Specifically, the working conditions referred to in para. c) above involve exposing workers to serious danger, considering the nature of the tasks to be performed and the working conditions.

Note that Art. 25-duodecies was amended by Law 161/2017, which introduced a reference to Art. 12 of Legislative Decree 286/1998 ('*Measures to combat illegal immigration'*), on the procurement of illegal entry of foreigners into the State and the aiding and abetting of illegal immigration. The revised Art. 25-duodecies references Art. 12 of Legislative Decree 286/1998, specifically paragraphs 3, 3-bis, 3-ter, and 5, which address the acts/conduct of anyone who '*manages, organises, finances or transports foreigners into State territory or commits other acts intended to obtain their illegal entry into the territory of the State',* or who facilitates their stay '*in order to generate an illegitimate gain or profit from their illegal status'*. Art. 12(3) of Legislative Decree 286/1998 was most recently amended by Decree-Law 20/2023, converted with modifications by Law 50/2023, which increased the penalty for the conduct outlined therein.

CHAPTER H.2

Sensitive Processes in the context of offences against personal dignity and recruitment of undocumented third country nationals

In relation to the predicate offences identified above, which trigger administrative liability under the Decree, the following activities pose the greatest risk in relation to the predicate offences covered in this Special Part:

- recruitment and management of human resources;
- assignment of contracts to third-party contractors.

CHAPTER H.3

General Principles of Conduct

The aim of this Special Part, with a view to preventing the commission of the offences considered herein, is that all Recipients of the Model should adhere to all procedures and principles that are directly or indirectly instrumental to preventing the offences that are outlined in this Special Part, which the Company has adopted as a fundamental safeguard to facilitate and promote its smooth operation, trustworthiness and reputation.

In particular, Recipients, depending on the type of relationship established with the Company, must adhere to the following principles of conduct:

1) to refrain from engaging in conduct that constitutes an offence under this Special Part;
2) to refrain from engaging in conduct that, while not constituting an offence *per se*, could potentially become one;
3) to conduct themselves honestly, transparently and collaboratively, in compliance with applicable laws and company procedures.

In relation to the direct employment of non-EU nationals,

- the Company adopts measures to ensure compliance with legal obligations on the employment of foreign workers without regular stay permits;
- the Company does not employ non-EU workers without a residence permit, or with a revoked or expired permit for which no renewal application has been submitted, as evidenced by the relevant postal receipt;
- the Company does not employ non-EU workers residing in Italy for tourism purposes only, even though they have the necessary declaration of presence.

CHAPTER H.4

Specific procedural principles

In order to implement the rules listed in the previous Chapter, the principles set out below must be adhered to, as well as the general principles contained in the General Part of this Model.

1) Selection and recruitment of personnel

a. When establishing employment relationships, the Company:

• always prioritises the protection of individuals' and workers' rights over any economic considerations;

• ensures that all workers are provided with dignified working conditions;

b. the Company adopts formal measures to ensure compliance with legal obligations on the employment of foreign workers without regular stay permits;

c. the Company does not employ third-country nationals without a residence permit, or with a revoked or expired permit for which no renewal application has been submitted, as evidenced by the relevant postal receipt;

d. the Company does not employ third-country nationals staying in Italy for tourism purposes only, even though they have the necessary declaration of presence;

e. where foreign nationals are hired who are resident in non-EU countries, the Company liaises with the competent authorities to obtain any documentation required in order to regularise the foreign worker’s lawful entry into Italy and to establish a regularised working relationship;

f. where foreign nationals are hired who are already residing in Italy, the Company ensures that they possess a valid residence permit or, in the case of an expired permit, that they have initiated the renewal process;

g. the Company ensures that the renewal or continuance of the employment contract or relationship is conditional on the maintenance/renewal of the residence permit, and that the employment relationship will be suspended if the residence permit should lapse, pending its renewal;

h. the Company ensures that where workers from a staff leasing agency are deployed, the relationship with the agency is governed by a written agreement that includes – among other things – the agency's obligation not to act contrary to the provisions of the Decree and to comply, where applicable, with the Model adopted by the Company.

2) ***Management of contracted activities***

When entering into contracts with companies that deploy unskilled labour (such as cleaning and maintenance companies):

a. the Company adopts measures to ensure that the contractor and subcontractor do not hire, for activities performed on the Company's behalf, non-EU nationals without a residence permit or with an irregular residence permit. To this end, the Company ensures that the following safeguards are included in procurement contracts:

i. the contractor's guarantee, when providing services to the Company, to employ only foreign workers legally residing in Italy who have a regular employment relationship;

ii. the contractor's commitment to provide a list, specifying the details, of employees who have been assigned to perform the contracted and subcontracted services for the Company and to notify any changes to this list with sufficient notice;

iii. the contractor's commitment to provide, at the time of contract signing and subsequently at intervals agreed by the parties, a copy of the social security/contributions compliance certificate (DURC), issued by the competent authorities, indicating the administrative status of the contractor and its subcontractors;

iv. the Company's right to request all documents necessary in order to fully and promptly examine the regular employment status of employees;

v. the contractor's obligation not to subcontract activities without the prior authorisation of the client;

vi. the contractor's obligation to enter into relationships only with subcontractors who are in a position to guarantee compliance with applicable labour laws, including laws on the recruitment of non-EU workers, under penalty of automatic termination of the procurement contract;

b. the Company adopts procedures for accessing the subcontractor's company premises, in order to ensure that workers from third-party companies engaged in continuous services for the Company can be identified, and to verify the identity of such individuals against the names provided.

CHAPTER H.5

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the scope of their respective duties and responsibilities, comply with the rules and principles set out in this Special Part.
In particular, the SB has the following duties:

- to monitor the effectiveness of the principles contained in company policies adopted for the prevention of offences outlined in this Special Part;

- to propose any necessary changes to Sensitive Processes attributable to potential changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The SB shall be promptly informed of any infringements of the specific procedural principles contained in this Special Part, infringements of company procedures, policies and standards touching on the Sensitive Processes identified above.
In relation to the employment of third-country nationals, the SB receives information on any recruitment of employees residing in non-EU countries.
The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART – I –

Tax offences

CHAPTER I.1

I.1.1. Tax offences (Art. 25-quinquiesdecies of Legislative Decree 231/2001)

This Special Part deals with the tax offences referenced in Art. 25-undecies of the Decree.

The Decree-Law no. 124 of 26 October 2019 entitled '*Urgent provisions on tax matters and for indispensable requirements',* converted with amendments by Law no. 157 of 19 December 2019, introduced Article 25-quinquiesdecies ('*Tax Offences'*) into the Decree.

Finally, Legislative Decree 87/2024 introduced further amendments to Article 25-quinquiesdecies, specifically adding paragraph 2-bis to Article 10-quater ('*Illegal offsetting of*

tax credits'), which allows for a specific exemption from punishment only where credits are illegitimately offset that are not in fact owing.

FRAUDULENT TAX RETURN USING INVOICES OR OTHER DOCUMENTS FOR NON-EXISTENT TRANSACTIONS (ART. 2 OF LEGISLATIVE DECREE 74/2000)

This offence committed by anyone who, in order to evade income tax or value added tax, using invoices or other documents for non-existent transactions, declares fictitious liabilities in a tax return related to those taxes.

The offence is deemed committed when such invoices or documents are recorded in mandatory accounting records or are held as evidence for tax purposes for the tax authorities.

A reduced penalty is provided if the amount of fictitious liabilities is less than EUR 100,000.

FRAUDULENT TAX RETURN USING OTHER STRATAGEMS (ART. 3 OF LEGISLATIVE DECREE 74/2000)

Outside the cases provided for in the previous article, this offence is committed by anyone who, in order to evade income tax or value added tax, by carrying out objectively or subjectively simulated transactions or by using false documents or other fraudulent means to hinder tax assessment and mislead the tax authorities, declares, in a tax return related to these taxes, a lower than accurate amount for assets or alternatively fictitious liabilities, credits and/or withholdings, when, together:

a) the tax evaded exceeds EUR 30,000 for any of the individual taxes;

b) the total amount of the assets withheld from taxation, including through the declaration of fictitious liabilities, exceeds 5% of the total amount of the assets indicated in the return, or exceeds EUR 1,500,000, or when the total amount of fictitious credits and withholdings reducing the tax exceeds 5% of the tax amount or, in any case, EUR 30,000.

The offense, too, is deemed to be committed with the use of false documents, when such documents are recorded in mandatory accounting records or are held as evidence for tax purposes for the tax authorities.

The term ‘fraudulent means’ does not include simple violation of the obligations to invoice and record assets in accounting records, or the simple indication in invoices or in accounting entries of assets at a value lower than their real value.

FALSE TAX RETURN (ART. 4 OF LEGISLATIVE DECREE 74/2000)

This offence is committed when, for the purpose of evading income tax or VAT, a taxpayer declares in an annual tax return for such taxes, assets at a value lower than their real value or declares non-existent liabilities, when, together:

a) the tax evaded exceeds, for any of the individual taxes, the sum of EUR 100,000; b) the total amount of assets withheld from taxation, including through the declaration of non-existent liabilities, exceeds 10% of the total amount of assets indicated in the tax return, or exceeds EUR 2,000,000.

For this purpose, the following are not taken into account: incorrect classification, the valuation of objectively existing asset or liability elements (provided that the criteria applied are indicated in the financial statements or in other relevant tax documentation), the violation of criteria for determining the relevant tax period, non-relevance, or non-deductibility of real liabilities. Valuations that differ, overall, by less than 10% from the correct ones shall not be punishable. This offence is relevant for the purposes of the Decree only if committed as part of cross-border fraudulent schemes linked to the territory of at least one other EU Member State and aimed at evading VAT for a total amount no less than EUR 10 million.

FAILURE TO MAKE A TAX RETURN (ART. 5 OF LEGISLATIVE DECREE 74/2000)

This offence is committed when, for the purpose of evading income tax or VAT, a taxpayer fails to file a mandatory tax return, and the tax evaded exceeds EUR 50,000 for any of the individual taxes.

This offence is also committed when a taxpayer, being obligated to do so, fails to file a withholding tax return, and the amount of unremitted withholdings exceeds EUR 50,000.

A return filed within 90 days of the deadline, or unsigned, or not drafted on the prescribed form is not considered omitted.

This offence is relevant for the purposes of the Decree only if committed as part of cross-border fraudulent schemes linked to the territory of at least one other EU Member State and aimed at evading VAT for a total amount no less than EUR 10 million.

ISSUANCE OF INVOICES OR OTHER DOCUMENTS FOR NON-EXISTENT TRANSACTIONS (ART. 8 OF LEGISLATIVE DECREE 74/2000)

This offence committed by anyone who, in order to enable third parties evade income tax or value added tax, issues invoices or other documents for non-existent transactions.

Paragraph 2 indicates that the issuance of multiple invoices or documents for non-existent transactions during the same tax period is considered a single offence.

A reduced penalty is provided if the incorrect amount indicated in the invoices or documents, for the tax period, is less than EUR 100,000.

CONCEALMENT OR DESTRUCTION OF ACCOUNTING DOCUMENTS (ART. 10 OF LEGISLATIVE DECREE 74/2000)

This offence is committed by anyone who, in order to evade income tax or VAT, or to facilitate third parties to evade them, conceals or destroys, in whole or in part, accounting records or documents whose retention is mandatory, in order to impede any reconstruction of income or turnover.

FRAUDULENT EVASION OF TAX PAYMENTS (ART. 11 OF LEGISLATIVE DECREE 74/2000)

The offence under para. 1 of this article is committed by anyone who, in order to evade the payment of income taxes or VAT or related interest or administrative penalties, for such taxes, which exceed EUR 50,000, fraudulently transfers or performs other fraudulent acts in relation to their own or others' assets, in such a way as to undermine the tax collection enforcement procedure, in whole or in part.

A more severe penalty is provided if the amount of taxes, penalties, and interest exceeds EUR 200,000.

The offence under para. 2 is committed by anyone who, in order to obtain a partial payment of taxes and related charges for themselves or others, declares, in documentation submitted in a tax settlement procedure, inappropriately low amounts for assets or fictitious liabilities for a total exceeding EUR 50,000.

A more severe penalty is provided if the amount of taxes, penalties and interest exceeds EUR 200,000.

ILLEGAL OFFSETTING OF TAX CREDITS (ART. 10-QUATER OF LEGISLATIVE DECREE 74/2000)

This offence is committed by anyone who fails to pay amounts due by offsetting credits, pursuant to Article 17 of Legislative Decree no. 241 of 9 July 1997, that are not owing or are fictitious, for an annual amount exceeding EUR 50,000.

This offence is relevant for the purposes of the Decree if committed as part of cross-border fraudulent schemes linked to the territory of at least one other EU Member State, and aimed at evading VAT for a total amount no less than EUR 10 million.

****

The aforementioned offences of filing a false tax return, failure to file a tax return and the illegal offsetting of tax credits were introduced into Article 25-quinquiesdecies of the Decree by Legislative Decree no. 75 of 14 July 2020 (implementing the PIF Directive), and subsequently amended by Legislative Decree 156/2022 entitled '*Corrective and supplementary provisions to Legislative Decree no. 75 of 14 July 2020, implementing Directive (EU) 2017/1371 on combating fraud to the detriment of the financial interests of the Union through the criminal law'*.

Specifically, under para. I-bis of Article 25-quinquiesdecies, these offences acquire relevance for the administrative liability of entities when they are '*committed as part of cross-border fraudulent schemes linked to the territory of at least one other EU Member State, and aimed at evading VAT for a total amount no less than EUR 10 million'*.

CHAPTER I.2

Sensitive Processes in the context of tax offences

The following are the main Sensitive Processes identified by the Company in relation to the offences covered in this Special Part, which the Company has identified within its organisation:

1. preparation of accounting records, tax returns, and management of tax compliance obligations;
2. storage of accounting records and other documents whose retention is required for tax purposes;
3. management of outgoing invoices;
4. management of incoming invoices;
5. management of deductible expenses;
6. VAT management;
7. management of mandatory periodic tax returns and tax calculations;
8. management of periodic payments.

CHAPTER I.3

General Principles of Conduct

The aim of this Special Part, with a view to preventing the commission of the offences considered therein, is to ensure that all Recipients of the Model comply with all the principles that are directly or indirectly functional to preventing conduct that could trigger the tax offences outlined above.

Recipients must adhere to the following principles of conduct:

1. to conduct themselves honestly, transparently and collaboratively, in compliance with applicable laws and company procedures, in all Sensitive Processes identified in this Special Part;
2. to facilitate the monitoring of compliance with the principles governing the insertion, keeping and archiving of accounting declarations relevant for tax purposes;
3. to properly store accounting records and other documents whose retention is required for tax purposes;
4. to implement the ‘segregation of roles’ in the management of company accounts and the process of preparing tax returns;

5. to ensure the utmost propriety in dealings with the tax administration and the utmost transparency in communicating data and information to it.

The Company, when paying sums that are owing as taxes or contributions, ensures that:

1. only actually existing credits are used for offsetting purposes;
2. only credits that are actually due are used for offsetting purposes.

CAPITOLO I.4

Specific procedural principles

In order to implement the rules listed in the previous Chapter, the principles set out below must be adhered to, as well as the general principles contained in the General Part of this Model.

1) Preparation of accounting records, tax returns, and management of tax compliance obligations

When drawing up accounting records, the Company adopts principles aimed at ensuring:

1. traceability of flows and identification of the figures responsible for transmitting accounting and financial data required for the preparation of accounting records;
2. proper storage of accounting records relevant for tax purposes;
3. compliance with the principle of segregation of duties and the involvement of different individuals when carrying out the main accounting activities (invoicing, bookkeeping, payment, archiving of documentation).

When drafting annual income tax and VAT returns, the Company adopts formal safeguards to ensure that:

1. asset items are not itemised at inappropriately low values, and fictitious liabilities are not itemised;
2. a taxable base is not declared which is lower than the applicable one (e.g. fictitious costs incurred and/or revenues declared at a value lower than the real value) by relying on false representation in mandatory accounting records and/or by using means aimed to obstruct the tax assessment process.

2) Storage of accounting records and other documents whose retention is required for tax purposes

The Company ensures that:

1. a copy of tax documents is also stored in digital format and protected by an adequate backup system and a disaster recovery procedure in case of cyberattacks or malfunctions of the Company's IT systems;
2. in case of inspections, all tax documents and accounting records are readily accessible and must be made transparently available to public officials.

3) Management of Invoicing

Outgoing and incoming invoicing processes are characterised by the principle of segregation of roles. Specifically, the Company, through multiple individuals, ensures that the following checks are carried out, both before issuing an invoice and upon receipt of third-party invoices (and, in any case, before making payments for the latter invoices):

1. verifying that the amounts indicated in invoices or other relevant documents correspond to the actual value of the goods/services purchased/sold;
2. verifying that the amounts indicated in invoices or other relevant documents correspond to the amount of the related payment;
3. verifying that the individuals indicated in invoices or other relevant documents correspond with the actual parties to the relationship described therein;
4. requesting and obtaining approval from the budget manager (who instigated the purchase) before making the payment, in relation to the amount of the invoice and also the appropriateness of the goods/services received;
5. verifying that a correspondence exists between the contract/purchase order, invoice and payment authorisation.

5) Management of financial and monetary flows

Reference is made, where applicable, to the provisions of **Special Parts A, B, and C**, particularly in relation to the ***Management of financial flows***.

All information acquired and financial transactions performed must be adequately traceable through the management systems in use, and capable of being reconstructed ex-post.

6) Management of dealings with the tax authorities

The Company is committed to ensuring the utmost collaboration and transparency in its dealings with the Italian tax authorities.

In particular, the Company ensures that:

1. individuals with specific authorisation to communicate with the Italian Tax Authority and respond to its requests are expressly identified;
2. any communication of information/data to the Italian Tax Authority is carried out correctly and exhaustively.

Chapter I.5

Controls by the Supervisory Body

The SB conducts periodic checks to verify that Recipients, within the scope of their respective duties and responsibilities, comply with the rules and principles set out in this Special Part.

In particular, the SB has the following duties:

- to monitor the effectiveness of the principles contained in company policies adopted for the prevention of offences outlined in this Special Part;
- to propose any necessary changes to Sensitive Processes attributable to potential changes in the Company's operations;
- to examine any special reports received from the audit/control bodies, from third parties or from any employee or key corporate officer, and to carry out any checks deemed necessary or appropriate in relation to the reports received.

The SB must be promptly informed of any violations of the specific procedural principles contained in this Special Part or of the company procedures, policies and standards touching on the Sensitive Processes identified above.

The SB also has authority to access, or to request its delegatees to access, any documentation and any company sites if pertinent to the performance of its duties.

SPECIAL PART - L -

Smuggling offences

CHAPTER L.1

The offences

This section of the Special Part refers to smuggling offences, as outlined in Article 25-sexiesdecies of the Decree (added by Legislative Decree 75/2020 and amended by Legislative Decree 141/2024). Specifically, it lists the individual offences considered relevant for the administrative liability of GIMA S.p.A.

Legislative Decree 141/2024, entitled '*National provisions complementary to the Union Customs Code and revision of the sanctions system for excise duties and other indirect taxes on production and consumption'*, approved the national provisions complementary to the Union Customs Code, reorganised customs regulations, repealed Presidential Decree 43/1973 (among others), and amended the text of Article 25-sexiesdecies of the Decree, dedicated to smuggling offences.

Among the novelties introduced by Legislative Decree 141/2024 is the inclusion of offences under the Consolidated Excise Law (Legislative Decree 504/1995) in the list of predicate offences (Article 18, paragraph II of Legislative Decree 141/2024), as well as the tightening of the sanctions regime for certain offences under Article 25-sexiesdecies. This includes the applicability of sanctions such as disqualification from conducting business activities and suspension or revocation of authorisations, licences, or concessions instrumental to the commission of the offence.

The new rules contained in the national provisions complementary to the Union Customs Code also provide for the application of criminal sanctions for smuggling when the threshold is exceeded of ten thousand euros in unpaid and undeclared, or incorrectly declared, customs duties.

The revised wording of Article 25-sexiesdecies further stipulates that a fine of up to four hundred units will be imposed where the taxes or one of the customs duties due exceed one hundred thousand euros.

Finally, in addition to the sanctions already provided for by the Decree, in cases of greater severity sanctions can be imposed such as disqualification from conducting business activities and suspension or revocation of authorisations, licences, or concessions instrumental to the commission of the offence.

Accordingly, this Special Part identifies the relevant Sensitive Processes (those in which an offence could in theory be committed and which have been identified within the risk assessment), specifying the principles of conduct and operational control safeguards to help organise, implement and manage operations carried out within the aforementioned Sensitive Processes.

ART. 78 SMUGGLING BY FAILURE TO MAKE A CUSTOMS DECLARATION

1. Anyone who engages in any of the following activities while failing to submit a customs declaration, shall be punished by a fine of between 100% and 200% of the customs duties due:

a) introduces and/or distributes non-Union goods within the customs territory or removes them from customs surveillance, in any manner and on any basis whatsoever;

b) causes Union goods to leave the customs territory, on any basis whatsoever.

2. The sanction referred to in para. 1 shall apply to anyone holding non-Union goods when the circumstances provided for in Article 19, paragraph 2, are met.

ART. 79 SMUGGLING BY MAKING A FALSE DECLARATION

1. Anyone who declares the quality, quantity, origin, and value of goods, and any other element required for the application of the tariff and for the calculation of duties, in a manner inconsistent with the known facts, shall be punished with a fine of between 100% and 200% of the customs duties payable or of the duties illegitimately received or unlawfully claimed for refund.

ART. 80 SMUGGLING OF GOODS BY SEA, BY AIR AND IN BORDER LAKES

1. The commander of an aircraft or captain of a ship shall be punished with a fine of between 100% and 200% of the customs duties owing, if they:

a) unload, load or transfer non-Union goods in the territory of the State without presenting them to the nearest Customs Agency office;

b) at the time of departure, do not have on board non-Union goods or goods for export with duty drawback, which should be present according to the terms of the manifest, the summary declaration and other customs documents;

c) transport non-Union goods into the territory of the State without being in possession of the manifest, the summary declaration and other customs documents where required.

2. The same penalty referred to in paragraph 1 shall also apply to:

a) a ship's captain who, in violation of the prohibition under Article 60, while transporting non-Union goods, skirts the national shores or drops anchor, lies to, or otherwise communicates with the territory of the State in such a way as to facilitate the landing or boarding of the goods;

b) an aircraft captain who, while transporting non-Union goods, lands outside a customs airport and fails to report the landing to the authorities indicated in Article 65, by the following working day. In such cases, the aircraft as well as its cargo shall be deemed to have been smuggled into the customs territory.

ART. 81 SMUGGLING FOR ILLEGITIMATE USE OF GOODS IMPORTED WITH TOTAL OR PARTIAL REDUCTION OF DUTIES

1. Anyone who assigns (in whole or in part) to non-Union goods imported with an exemption from or reduction of duties, a designation or use other than that for which the duty-free status or reduction was granted, shall be punished with a fine of between 100% and 200% of the customs duties owing.

ART. 82 SMUGGLING WHEN EXPORTING GOODS ELIGIBLE FOR DUTY DRAWBACK

1. Anyone who uses fraudulent means to illegitimately obtain a duty drawback established for the import of raw materials used in the manufacture of goods that are exported, shall be punished with a fine of between 100% and 200% of the amount of the duties illegitimately collected or sought to be collected.

ART. 83 SMUGGLING DURING TEMPORARY EXPORT AND IN SPECIAL USE AND PROCESSING PROCEDURES

1. Anyone who, during temporary export operations and in special use or processing procedures, in order to evade the payment of customs duties that would be payable, subjects the goods to artificial manipulations or uses other fraudulent means, shall be punished with a fine of between 100% and 200% of the customs duties owing.

ART. 84 SMUGGLING OF PROCESSED TOBACCO PRODUCTS

1. Anyone who introduces, sells, distributes, purchases or holds, on any basis whatsoever, in the territory of the State, a quantity of smuggled processed tobacco exceeding 15 conventional kilograms, as defined by Article 39-quinquies of the Consolidated Law under Legislative Decree 504 of 26 October 1995, shall be punished by a term of imprisonment ranging from two to five years.

2. The acts referred to in paragraph 1, when involving a quantity of processed tobacco up to 15 conventional kilograms only, and in the absence of the aggravating circumstances referred to in Article 85, shall be punished with an administrative fine of EUR 5 for each conventional gram of product, in any case not less than EUR 5,000.

3. If the quantities of smuggled processed tobacco products:

a) do not exceed 200 conventional grams, the administrative fine shall in any case be EUR 500;

b) range between 200 and 400 conventional grams, the administrative fine shall in any case be EUR 1,000.

ART. 85 AGGRAVATING CIRCUMSTANCES OF THE OFFENCE OF SMUGGLING OF PROCESSED TOBACCO PRODUCTS

1. If the acts provided for in Article 84 are committed using means of transport belonging to persons not involved in the offence, the penalty shall be increased.

2. In the cases provided for in Article 84, a fine of EUR 25 for each conventional gram of product and a term of imprisonment ranging from three to seven years shall be imposed, whenever:

a) while committing the offence or in actions aimed at securing the price, product, profit or impunity of the offence, the perpetrator uses weapons or is found to have possessed them during the commission of the offence;

b) while committing the offence or immediately thereafter, the perpetrator is caught together with two or more persons in circumstances such as to obstruct the law enforcement agencies;

c) the illegal act/conduct is linked to another offence against the public trust or against the public administration;

d) while committing the offence, the perpetrator has used means of transport which, have altered or modified the approved characteristics in a manner likely to obstruct the intervention of the law enforcement agencies or to cause a danger to public safety;

e) while committing the offence, the perpetrator has availed of partnerships or companies or has made use of financial resources in any manner established in States that have not ratified the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, signed in Strasbourg on 8 November 1990, ratified and implemented by Italian Law no. 328 of 9 August 1993, and that, in any case, have not concluded and ratified judicial assistance agreements with Italy in the field of smuggling offences.

ART. 86 CRIMINAL ASSOCIATION AIMED AT SMUGGLING OF TOBACCO PRODUCTS

1. When three or more persons associate in order to commit multiple offences under Article 84 or Article 40-bis of the Consolidated Law of legislative provisions on taxes on production and consumption and related criminal and administrative sanctions, referred to in Legislative Decree no. 504 of 26 October 1995, including with reference to the products referenced in Articles 62-quater, 62-quater.1, 62-quater.2, and 62-quinquies of the said Consolidated Law,

the persons who promote, establish, direct, organise or fund the association shall be punished, by these acts alone, by a term of imprisonment ranging from three to eight years.

2. Anyone who participates in the association shall be punished by a term of imprisonment ranging from one to six years.

3. The penalty shall be increased if the number of associates is ten or more.

4. If the association is armed or if the circumstances are present which are provided for in Article 85, paragraph 2, letters d) or e), or in Article 40-ter, paragraph 2, letters d) or e), of the aforementioned Consolidated Law under Legislative Decree No. 504 of 1995, including with reference to the products referenced in Articles 62-quater, 62-quater.1, 62-quater.2, and 62-quinquies of the same Consolidated Law, a term imprisonment ranging between five and fifteen years shall be imposed in the cases provided for in paragraph 1, and between four and ten years in the cases provided for in paragraph 2. The association shall be considered armed if the participants have the availability of weapons or explosive materials in order to achieve its purposes, even if concealed or kept in storage.

5. The penalties provided for in Article 84 and in this Article shall be reduced by one-third to one-half in the case of a perpetrator who, dissociating themselves from the others, takes steps to prevent the criminal activity from resulting in further consequences, including by giving concrete assistance to the police or judicial authorities in gathering evidence that proves decisive in reconstructing the facts and in identifying or capturing the perpetrators, or in identifying resources relevant to the commission of the criminal offences.

ART. 88 AGGRAVATING CIRCUMSTANCES OF THE OFFENCE OF SMUGGLING

1. For the offences provided for in Articles 78 to 83, anyone who, in order to commit smuggling, uses means of transport owned by a person not involved in the offence is liable to a fine increased by up to one half.

2. For the offences referred to in paragraph 1, a term of imprisonment ranging from three to five years shall be added to the fine:

a) if the perpetrator is found armed while committing the offence or immediately thereafter, in the surveillance zone;

b) if three or more persons are found together while committing the smuggling offence or immediately thereafter, in the surveillance zone, in circumstances that obstruct law enforcement agencies;

c) if the offence is linked to another criminal offence against the public trust or against the public administration;

d) if the perpetrator is an associate for the purpose of committing smuggling offences and the offence committed is among those for which the association was established;

e) if the amount of at least one of the customs duties owing, considered separately, exceeds EUR 100,000.

3. For the offences referred to in paragraph 1, a term of imprisonment up to three years shall be added to the fine if the amount of at least one of the customs duties owing, considered separately, exceeds EUR 50,000 but does not exceed EUR 100,000.

ART. 94 RECOVERY OF ASSETS. CONFISCATION

1. In smuggling cases, the confiscation of the items that served or were intended to be used to commit the offence, and of the items that are the purpose, product or proceeds thereof, is always ordered. When it is not possible to confiscate the items referenced in the first sentence, the confiscation shall be ordered of sums of money, assets, and other earnings of equivalent value, which are available to the convicted person, including through an intermediary.

2. Also subject to confiscation are any means of transport, owned by whomever, that have been adapted for the fraudulent stowing of goods or that contain devices capable of increasing their loading capacity or range, contrary to approved construction specifications, or that are used in violation of the rules of traffic or navigation and safety at sea.

3. The provisions of Article 240 of the Penal Code shall apply if the means of transport belongs to a person not involved in the offence, if that person proves that they could not have foreseen its unlawful use, even occasionally, and that they were not guilty of a lack of vigilance.

4. The provisions of this article shall also apply where a plea is made for a sentence applying punishment at the request of the parties under Book VI, Title II, Article 444 of the Code of Criminal Procedure.

5. In cases of criminal conviction, or where a plea is made for a sentence applying punishment at the request of the parties pursuant to Article 444 of the Code of Criminal Procedure for any of the offences provided for in Article 88(2), the provisions of Article 240-bis of the Penal Code shall be applicable.

CHAPTER L.2

Identification of activities vulnerable to offence risk

After the risk mapping phase, 'at-risk areas' were identified i.e. operations and processes and areas within the Company where there is deemed to be a potential risk of commission of smuggling offences under the Decree.

Before examining these areas and the related control measures and safeguards, it is important to note that – as emerged during the risk assessment and risk analysis activities – the Company carries out significant imports of goods from non-EU countries and typically entrusts all import and customs clearance operations to specialist customs brokers, who assist the Company in preparing customs forms, calculating customs duties and making the required payments.

That said, the activities that the Company has identified as Sensitive Processes, in the context of smuggling offences, are detailed in the Matrix of At-Risk Activities, along with potential examples of purposes and methods of committing the offences in question.

These activities are summarised below:

- management of goods import and export activities;
- management of dealings with customs brokers and carriers operating on behalf of the Company, and of their professional credentials;
- identification and selection of suppliers of goods and/or services, i.e. business partners from whom to source;

- management of dealings with the Italian Customs and Monopolies Agency (ADM) in the context of import and export activities, including through third parties (e.g. customs brokers/carriers etc.);
- keeping of documentation suitable for tracking goods.

CHAPTER L.3

General Principles of Conduct

In line with the corporate ethical principles set out in the General Part of the Model, pursuant to the Decree, all Recipients of the Model must, when carrying out the Sensitive Processes mentioned above, observe the conduct and control principles set out below.

Recipients are in general forbidden from:

- engaging with the Italian Customs and Monopolies Agency ('Customs Agency', below) on behalf of or representing the Company, without a special delegated authority from the Company for this purpose;
- submitting declarations, communications or documents containing untrue, misleading or partial information to the Customs Agency, or omitting information, in order to obtain favourable decisions from the Customs Agency;
- providing false documents or information to customs brokers and/or the Customs Agency;
- engaging in deceptive or fraudulent conduct with members of the Customs Agency, thereby leading the latter into errors of judgement;
- granting professional assignments, giving or promising gifts, money or other economic benefits to persons responsible for carrying out customs inspections and checks;
- obtaining, importing, exporting, concealing, unloading, storing or holding goods in violation of customs regulations.

In accordance with the Code of Ethics and with corporate procedures, Recipients are also obliged:

- to ensure that all relevant corporate, accounting, customs and tax documentation are properly prepared, maintained and retained. Therefore, there is a strict prohibition against any

conduct that, by failing to promptly update, improperly store or conceal documents, prevents relevant supervisory authorities and bodies from carrying out the necessary control activities;

- to pay or ensure their payment of duties owing;
- to ascertain the identity of the counterparty and any parties on whose behalf they may be acting.

Furthermore:

- corporate procedures are characteristically divided into separate decision-making, execution and control functions, with adequate formalisation and documentability of the main stages of the process;
- all relationships with public officials must be characterised by honesty and formality, and be mindful of the multiple implications that such a relationship may give rise to;
- external parties delegated to deal with and represent the Company before the Customs Agency, also during the latter's inspections and audits, are formally identified, and their delegated powers (or professional assignments) are formalised in writing;
- there is continuous monitoring of legislative and regulatory changes and of the deadlines for communications, reports and compliance obligations vis-a-vis the Customs Agency, including with the assistance of external consultants;
- documentation (on paper or electronic media) related to the management of customs compliance obligations and checks/controls carried out, is filed and stored in a dedicated paper/digital archive;
- customs brokers are selected based on reputation, integrity and reliability, from among entities registered in the professional register of licensed customs brokers;
- customs brokers are evaluated and included in the supplier database based on their ability to meet the requirements demanded by the type of product being supplied and the scale of the supply (e.g. destination country);
- when selecting customs brokers, the broker's integrity and commercial reliability are checked, and such checks are duly documented;
- to ensure the segregation of duties, a distinction is made between persons who issue purchase orders and prepare contracts, persons who verify the correct receipt of goods or the successful provision of services, and the persons who authorise the invoice for payment;
- contracts/purchase orders and engagement letters with customs brokers provide information about the Company's standards of conduct adopted in connection with the

Organisational Model and Code of Ethics, and about the implications, for the future of the contractual relationship, of conduct that violates the provisions of the Code of Ethics and the Company's norms of conduct and infringes applicable legislative and regulatory provisions.

CHAPTER L.4

Specific procedural principles

1) management of import/export activities

a) identifying roles and responsibilities connected with import/export activities;
b) verifying that the necessary permits from the public authorities are obtained and kept valid, for purposes of importing, transporting, exporting, holding and storing merchandise;
c) ensuring that procedures are in place for verifying the entry and exit of goods which include verifying customs documents and any other documents required for tax processing;
d) for imports, verifying that the order is consistent with the goods actually imported;
e) for exports, verifying that the order is consistent with the goods prepared for shipment.

2) management of logistics and goods transit activities

a) identifying roles and responsibilities related to inbound/outbound logistics processes;
b) ensuring that goods received are checked for quantity and quality conformity, for origin, and for any applicable special tax or customs arrangements (e.g. incentives, benefits) are verified;
c) ensuring that movements of goods between the company's various warehouses/sites/depots are traceable;
d) verifying that transport documents/accompanying documents comply with current industry regulations (for the aspects handled by the company).

Chapter L.5

Duties of the Supervisory Body

In relation to the need to prevent the risk of commission of the offences referenced in this Special Part, the Supervisory Body is tasked with:

- monitoring the adequacy and effectiveness of the Model and its associated prevention protocols, and of the Code of Ethics, of current procedures and of the system of powers of attorney and delegated powers;
- identifying any shortcomings in the Model, and also any non-compliant behaviour; it is also tasked with conducting any checks and verifications deemed appropriate or necessary, and with informing the competent bodies of any violations found, in conformity with the Disciplinary System adopted under the Decree;
- ensuring the updating of the Model by proposing improvements/adjustments aimed at ensuring that its provisions are adequate and/or effective.

The Supervisory Body must report the results of its monitoring and control activities to the management body, in accordance with the terms and procedures set out in the Model.