ITALFARMACO S.P.A.

ORGANISATION MANAGEMENT AND CONTROL MODEL

IN COMPLIANCE WITH ITALIAN LEGISLATIVE DECREE

NO. 231 OF 8 JUNE 2001

updated on September 29 -2025

GENERAL PART

DEFINITIONS

SENSITIVE ACTIVITIES: operations or actions that could expose the COMPANY to the risk of committing any of the offences provided by the DECREE;

BOD: Board of Directors;

CODE OF ETHICS: Code adopted by means of Board of Directors' resolution of 28 May 2010, as amended;

DECREE: Italian Legislative Decree no. 231[1] of 8 June 2001, according to its current wording;

RECIPIENTS: the individuals to whom the provisions of the MODEL apply;

COMPANY REPRESENTATIVES: The Chairman and members of the Board of Directors, the Board of Statutory Auditors, the General Managers, the members of any other corporate bodies that the COMPANY may have established pursuant to Article 2380 of the Italian Civil Code or special laws, as well as any other individual in a senior position pursuant to the Decree. This is understood to mean any person who performs representative, administrative or managerial functions within the Company or a unit or division thereof, with financial and functional autonomy;

EMPLOYEES: individuals who are in employment relationships with the COMPANY, of any level or any nature, including workers on fixed-term contracts, placement contracts, apprenticeship contracts or part-time contracts, as well as workers on secondment or so-called para-subordinate contracts (supply of work);

[1] And subsequent additions and amendments: this clarification applies to any law, regulation or set of regulations referred to in the MODEL.

COLLABORATORS: individuals who, in relation to the COMPANY, are in (i) project-based employment contracts; (ii) agency relationships and other relationships that constitute the provision of coordinated, continued and predominantly individual work on a non-subordinate basis; (iii) relationships of occasional collaboration (e.g. consultancy), as well as individuals subject to the management or supervision of a COMPANY REPRESENTATIVE;

SUPPLIERS: any entity that provides the COMPANY with goods or services;

ELECTRONIC DOCUMENT: any electronic medium containing data or information of probative force or programmes specifically designed to process such data or information;

ADMINISTRATIVE OFFENCES: the offences pursuant to Italian Legislative Decree 231/2001, as amended;

GUIDELINES: the FARMINDUSTRIA Guidelines;

MODEL: this Organisation, Management and Control Model as provided for by Italian Legislative Decree 231/2001, as amended;

CORPORATE BODIES: the Board of Directors, the Managing Director, and the Board of Statutory Auditors;

COMMITTEE: the Compliance Committee provided for by Italian Legislative Decree 231/2001;

PA: the Public Administration;

Crimes: Crimes referred to in Articles 24, 24-*bis*, 24-*ter,* 25, 25-*bis*, 25-*bis*.1, 25-*ter*, 25-*quater*, 25-*quater.1,* 25-*quinquies,* 25-*sexies,* 25-*septies*, *25-octies, 25-octies.1,* 25-*novies*, 25-*decies,* 25-*undecies*, 25-*duodecies,* 25-*terdecies*, 25-*quaterdecies,* 25-*quinquesdecies*, 25-*sexiedecies , 25-septiesdecies, 25-*

duodevicies and 25-undevicies of Italian Legislative Decree no. 231 of 8 June 2001, and the offences pursuant to Law no. 146 of 16 March 2006, ratifying and implementing the United Nations Convention against Transnational Organized Crime, which the UN General Assembly adopted on 15 November 2000 and on 31 May 2001; ;

DISCIPLINARY SYSTEM: the collection of penalties applicable in cases of breaches of the MODEL;

COMPANY: Italfarmaco S.p.A.;

GROUP: the group of businesses controlled by the COMPANY;

SENIOR EXECUTIVES: individuals who perform representative, administrative or managerial functions in the COMPANY, or any of its units that has financial and functional autonomy, as well as individuals who manage and control them, including on a de facto basis;

TABLE OF CONTENTS

CHAPTER I

ITALIAN LEGISLATIVE DECREE 231/2001: SUMMARY OF THE LEGISLATION

Chapter II

THE ITALFARMACO S.P.A. MODEL

GENERAL PART

CHAPTER III

THE ITALFARMACO S.P.A. MODEL

SPECIAL PART

CHAPTER I

ITALIAN LEGISLATIVE DECREE 231/2001: SUMMARY OF THE LEGISLATION

1. Italian Legislative Decree no. 231/2001 and reference legislation

Italian Legislative Decree no. 231 of 2001 [2] adapted Italian legislation to international Conventions on the liability of legal persons[3].

The Decree introduced the concept of the liability of organisations (legal persons and associations) deriving from offences: direct liability of an administrative nature arising from the commission of offences by figures functionally linked to the organisation.

2. Nature and characteristics of the liability of legal persons

The liability of organisations is additional to, but does not replace, the liability of the natural person who committed the offence.

Liability exists even if the perpetrator of the offence has not been identified, or the offence has lapsed for a reason other than amnesty.

Administrative penalties against the organisation lapse after a period of five years from the date on which the offence was committed. However, if said period is interrupted due to the occurrence of one of the expressly specified acts, the period recommences without any maximum limit. Therefore, the offence may lapse, but the organisation can still be held liable.

3. Offences identified by the DECREE, as amended

The organisation's liability only emerges in the cases and within the limits explicitly

[2] The DECREE was published in the Italian Official Gazette no. 140 of 19 June 2001, and entered into force on 4 July 2001.

[3] Such as the Brussels Convention of 26 July 1995, on the protection of the European Communities' financial interests; the Convention of 26 May 1997, on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union; the OECD Convention of 17 December 1997, on combatting bribery of foreign public officials in international business transactions and related instruments.

provided for by law: the organisation "*cannot be held liable for an act that constitutes an offence, if its liability (...) and the relative penalties are not explicitly provided for by a law*" that entered into force before the commission of the offence.

Therefore, the organisation can only be held liable for the commission of crimes and administrative offences that are provided for by the Decree and the laws that refer to the provisions thereof.

Italian Law no. 146 of 16 March 2006, on the ratification and enforcement of the United Nations Convention and Protocols against transnational organised crime[4] introduces the liability of organisations for some transnational criminal conduct.

Pursuant to Article 3 of that Law, offences committed by "*an organised crime syndicate*" are transnational in the following cases:

- when they are "*committed in more than one State*";
- when they are "*committed in one State, but a substantial part of their preparation, planning, management or control*" takes place "*in another State*";
- when they are "*committed in one State, but an organised crime syndicate, involved in criminal activity in more than one State, is implicated in them*";
- when they are "*committed in one State*", but have "*substantial effects in another State*".

4. Objective criteria for the attribution of liability

The DECREE provides criteria for the objective and subjective attribution of liability to the organisation.

The first criterion for attributing liability on an objective basis constitutes the commission of a crime or administrative offence "*in the interests or to the advantage of the organisation*".

The act is deemed to be in the interests of the organisation when it is committed for the

[4] The UN General Assembly adopted the Convention on 15 November 2000 and the protocols on 31 May 2001.

purposes of benefiting it[5]. The achievement of the objective being pursued is completely irrelevant.

The criterion of advantage, on the other hand, relates to the positive outcome that the organisation has objectively obtained from the commission of the offence, regardless of the perpetrator's intention.

The organisation is not held liable if the unlawful act is committed "*in the exclusive interests*" of the perpetrator or third parties. Therefore, liability arises if the interest is shared by the organisation, or partly pertains to it.

A second objective criterion for the attribution of liability is represented by the typology of the perpetrator of the offence.

The Decree provides for two categories of qualifying individuals:

- "*persons who perform representative, administrative or managerial functions within the organisation or one of its organisational units with financial and functional autonomy*" or those who "*manage and control*" the organisation "*including on a de facto basis*" (so-called individuals in "*senior positions*");
- "*persons subject to the management or supervision of a senior executive*" (so-called "*subordinates*").

Persons in "*senior positions*" are the legal representative, director and general manager of an office or branch, as well as the individuals who manage and control the organisation, including on a de facto basis[6].

"*Subordinates*" are the employees and workers external to the organisation to whom a task is entrusted under the management and supervision of senior executives.

5. For the purposes of the objective attribution of the offence, it is sufficient for the classified individual to provide a causal contribution to the commission of the offence, pursuant to Article 110 of the Italian Criminal Code. **Subjective criteria for the attribution of liability**

The DECREE defines the organisation's liability as direct, of its own account and culpable.

[5] The purpose does not need to be exclusive.

[6] So-called de-facto directors (Article 2639 of the Civil Code) or sovereign partners.

Liability is not attributed when, before the commission of the offence, the organisation has adopted and effectively implemented an *Organisation and Management Model* capable of preventing the commission of offences of the type that has occurred.

Accordingly, the organisation's liability is based on so-called "*organisational culpability*", or a lack of preventive adoption or compliance with standards pertaining to the entity's organisation and activity for the purpose of preventing offences. A failure to adopt the *Organisation and Management Model* gives rise to the presumption of culpability.

6. Offences committed by "*senior*" executives

For offences committed by individuals in "*senior*" positions, the DECREE establishes a presumption relating to the organisation's liability. It provides for the exclusion of liability only if it is demonstrated that the following combination of conditions are all met:

- "*the governing body has, before the commission of the offence, adopted and effectively implemented organisation and management models capable of preventing the commission of offences of the type that has occurred*";
- "*the task of supervising the functioning of and compliance with the models, and ensuring that they are updated, was entrusted to a body, within the organisation, that has autonomous powers of initiative and control*";
- "*the individuals committed the offence by fraudulently eluding the organisation and management models*";
- "*the committee with autonomous powers of initiative and control performed its compliance responsibilities or performed them adequately*".

7. Offences committed by individuals in "*subordinate*" positions

The organisation can only be held liable for offences committed by "*subordinates*" if it is established that "*the commission of the offence was made possible by a failure to perform managerial or*

supervisory obligations" attributed by law to individuals in a senior position or transferred to other individuals by delegation.

The failure to perform such obligations does not entail liability for the organisation "*if the organisation, before the commission of the offence, has adopted and effectively implemented an organisation, management and control model capable of preventing offences of the type that has occurred*". The adoption and implementation of a suitable organisation model therefore exempts the organisation from liability.

8. The characteristics of the "*Organisation and Management Model*"

The Decree does not govern the nature or characteristics of the model; it merely establishes some general principles which differ in relation to the typology of the perpetrator of the offence.

For the prevention of offences by "*senior executives*", the model must:

- "*identify the activities in the context of which offences may be committed*" (referred to as the mapping of risks);
- "*provide for specific protocols aimed at planning training and decision-making within the organisation, in relation to the offences to be prevented*";
- "*identify procedures for the management of financial resources that are able to prevent the commission of offences*";
- "*provide for reporting obligations in relation to the committee responsible for overseeing the functioning of and compliance with the models*";
- "*introduce a disciplinary system that is capable of penalising failures to comply with the measures outlined in the model*".

As regards offences that can be committed by individuals in "*subordinate*" positions, the model must establish, "*in relation to the nature and size of the organisation, as well as the type of activity carried out, measures that are able to guarantee that the activities will be carried out in compliance with the law and that risk situations will be discovered and eliminated in a timely manner*".

The following must be adopted for the effective implementation of the *Organisation, Management and Control Model*:

- "*a periodic check and any amendment when significant violations of the provisions are discovered or when changes are made to the organisation or its activities*";
- "*a disciplinary system capable of penalising failures to comply with the measures specified in the model*".

9. Offences committed abroad

Pursuant to Article 4 of the DECREE, the organisation is liable for the commission of some offences abroad where the following conditions are met:

- the offence is committed by an individual who is functionally linked to the organisation;
- the organisation has its main headquarters in the territory of the Italian state;
- the conditions provided for by Articles 7, 8, 9 and 10 of the Italian Criminal Code are met: where the law provides that the perpetrator of the offence should be punished at the request of the Ministry of Justice, action is brought against the organisation even if the request is made by it;
- the Authorities of the State in which the offence was committed do not bring action against the organisation.

10. Attempted offences

Administrative liability also arises in the event that the offence is committed in the form of an attempt (Article 56 of the Italian Criminal Code).

With reference to tax offences (referred to in Article *25-quinquiesdecies* of Legislative Decree no. 231/2001), although according to Article 6 of Legislative Decree no. 74/2000, the unlawful conduct does not assume criminal relevance at the level of attempt only, with the transposition of Directive (EU) 2017/1371 (the so-called "PIF Directive"), the conduct referred to in Articles 2, 3 and 4 of Legislative Decree no. 74/2000, even if carried out in the attempted form, only if the following four conditions are met:

1. the evasion must relate to a qualified amount,
2. the evasion must relate only to value added tax,
3. must be transnational facts affecting several EU states,

4. the contested act must not constitute the offence provided for in Article 8 of Legislative Decree 74 of 2000.

11. Penalties

The penalty system provided for by the DECREE establishes pecuniary and restrictive penalties.

11.1. Pecuniary penalties

If the organisation's liability is established, then pecuniary penalties are always applied. The penalty is ordered by the criminal judge when the liability derives from a criminal offence. It is imposed by the administrative authority in cases in which the organisation is being held liable for an administrative offence.

The penalties are determined by means of a "*quota-based*" system: a minimum and maximum number of quotas are provided for every offence. The judge establishes the number and monetary value of the quotas so as to ensure the penalty's effectiveness, taking account of the "*organisation's economic and financial*" conditions.

Pecuniary penalties are reduced:

- where the perpetrator of the offence predominantly committed the act in his/her own interests or the interests of third parties and the organisation obtained no advantage or a minimal advantage;
- where the damage caused is particularly minor.

The penalty is reduced by one third to one half if, before the first-instance hearing is declared open:

- the organisation has fully compensated the damage and eliminated the prejudicial or dangerous consequences of the offence, or taken action to do so;
- a model capable of preventing the commission of further such offences has been adopted and entered into operation.

In cases of offences under Article 25-*sexies* of the DECREE, if the result or profit obtained by the organisation is of significant value, the pecuniary penalty is increased by up to ten times such result or profit.

11.2. Restrictive penalties

Restrictive penalties are applied in addition to pecuniary penalties:

Those provided for by the DECREE are as follows:

- temporary or permanent disqualification from carrying on the business;
- the suspension or revocation of authorisations, licenses or concessions that were functional to the commission of the offence;
  the prohibition of entering into contracts with the public administration, except in order to obtain the provision of a public service;
- exclusion from grants, loans, contributions or subsidies and the potential revocation of any that have already been granted;
- temporary or permanent prohibition from advertising goods or services.

Restrictive penalties are only applied in the cases expressly provided for, provided that at least one of the following conditions are met:

- the organisation has obtained a significant profit from the offence, the commission of which was brought about or facilitated by severe organisational failings;
- in the event of repeated offences.

Restrictive penalties are normally temporary, but they can be applied permanently on an exceptional basis.

At the request of the public prosecutor, the judge can also apply restrictive penalties on a precautionary basis, where the following combination of conditions are all met:

- there is significant evidence of the organisation's liability;
- there is well-founded and specific evidence to suggest that there is a material danger that more offences, of the same type as those for which action is being brought, will be committed.

Pecuniary penalties are not applied (or are revoked, if applied on a precautionary basis) if, before the first-instance hearing has been declared open, the organisation has:

- compensated or repaired the damage;
- eliminated the prejudicial or dangerous consequences of the offence, or has taken action to do so;
- offered the profit obtained from the offence to the judicial authority for confiscation;

- eliminated the organisational shortcomings that led to the offence, adopting models designed to prevent the commission of new offences.

Only the pecuniary penalty will be applied in the above cases of so-called "*active remediation*".

11.3. Other penalties

The DECREE provides for another two penalties:

- confiscation, which consists of the State's acquisition of the price of or profit from the offence (or, when it is not possible to enforce this directly, the seizure of sums of money, assets or other items of an equivalent value), without prejudice to the compensation of the damage;
- the publication of the judgment of conviction, in summary form or in its entirety, at the organisation's expense, in one or several newspapers specified by the judge, and its display in the municipality where the organisation has its main headquarters.

12. Events which modify the organisation

The DECREE governs the organisation's liability in cases of events which modify it (transformations, mergers, demergers and transfers of business units).

In general terms, it is established that "*only the organisation is held liable for the obligation to pay the pecuniary penalty, with its own capital or mutual fund*".

The direct pecuniary liability of shareholders and partners is therefore excluded.

For the application of pecuniary penalties, the criteria established by the civil laws on the liability of organisations subject to transformation for the debts of the original organisation are applicable.

Restrictive penalties remain in effect against the organisation which has retained (or been assigned) the business unit within which the offence was committed. The organisation's power to obtain the conversion of the restrictive penalty into a pecuniary penalty remains without prejudice, provided that the organisational failings that made the commission of the offence possible have been eliminated.

12.1. Transformation

The Decree provides that, in cases of the "*transformation of the organisation, liability for offences committed prior to the date on which the transformation took effect remains without prejudice*".Therefore, changes to the legal structure (company name, legal form, etc.) are irrelevant: the new organisation will be the recipient of the penalties applicable to the original organisation.

12.2. Mergers and demergers

The organisation resulting from the merger, including mergers by acquisition, "*is held liable for offences for which the organisations participating in the merger were liable*". If the merger took place before the end of the proceedings to ascertain liability, the judge must take account of the economic condition of the original organisation, not the organisation resulting from the merger.

In the event of partial demergers through the transfer of part of the assets of the demerged company, which continues to exist, the organisation's liability for offences committed previously remains without prejudice.

Collective organisations that emerge as the beneficiaries of the demerger are obliged, on a joint and several basis, to pay the pecuniary penalties due from the demerged organisation, limited to the value of the assets transferred. This limit is not applicable for beneficiary organisations that have received all or part of the business unit within which the offence was committed.

12.3. Transfers and disposals

In the event of the transfer or disposal of the business unit in which the offence was committed, the transferee is obliged to pay the pecuniary penalty on a joint and several basis with the transferring organisation, limited to the value of the transferred business unit. The transferring organisation's right to prior discussion [*beneficium excussionis*] remains without prejudice.

The transferee's liability is limited to the pecuniary penalties resulting from its mandatory accounting records.

13. The catalogue of criminal offences

As to the offences to which the rules under review apply, these are currently the following types: (a) offences committed in dealings with the Public Administration and against the assets of the State or other Public Entity or of the European Union, (b) offences relating to counterfeiting money, public credit cards, revenue stamps and identification instruments or signs (c) corporate offences (including offences of bribery among private individuals and incitement to bribery among private individuals), (d) offences with the purpose of terrorism and subversion of the democratic order, (e) female genital mutilation practices, (f) offences against the individual, (g) offences of abuse or illegal communication of inside information. Recommendation or inducement of others to commit insider trading and market manipulation, (h) offences committed in breach of the rules on accident prevention and protection of hygiene and health at work, (i) handling stolen goods, money laundering, use of money, goods or benefits of unlawful origin as well as self laundering, (j) offences relating to non-cash means of payment and fraudulent transfer of values (k) transnational offences, (l) computer crimes and unlawful processing of data, (m) offences relating to violation of copyright, (n) offences against industry and trade, (o) organised crime offences, (p) offences against the administration of justice, (q) environmental offences, (r) offences relating to immigration and the status of foreigners, (s) racism and xenophobia offences (t) offences of fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited devices; (u) tax offences; (v) smuggling offences, (w) offences against cultural heritage; (x) laundering of cultural goods and devastation and looting of cultural and landscape heritage, (y) (crimes against animals).

Specifically, the offences, detailed in Annex 1, to which the discipline applies are the following:

a) OFFENCES COMMITTED IN RELATIONS WITH THE PUBLIC ADMINISTRATION AND AGAINST THE ASSETS OF THE STATE OR OTHER PUBLIC BODY OR OF THE EUROPEAN UNION (ARTICLES 24 AND 25):

   1) embezzlement of public funds (of the State or other public body or the European Union);

   2) undue receipt of of public funds (of the State or other public body or the European Union);

3) disturbed freedom of enchantments;
4) disturbing the freedom of choice of contractor procedure;

5) fraud in public procurement to the detriment of the State or other public body or the European Union;

6) fraud against the State or other public body or the European Union;

7) aggravated fraud to obtain public funds to the detriment of the State or other public body or the European Union;

8) computer fraud to the detriment of the State or other public body or the European Union;

9) fraud against the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development;

10) embezzlement to the detriment of the financial interests of the European Union;

11) misappropriation of money or movable property to the detriment of the financial interests of the European Union;

12) embezzlement by profiting from the error of others to the detriment of the financial interests of the European Union;

13) concussion;

14) corruption for the exercise of the function;

15) bribery for an act contrary to official duties;

16) bribery in judicial acts;

17) undue inducement to give or promise benefits;

18) bribery of a person entrusted with a public service;

19) incitement to corruption;

20) embezzlement, misappropriation of money or movable property, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery of members of international courts or bodies of the European Communities or of international parliamentary assemblies or international organisations and of officials of the European Communities and of foreign States;

21) trafficking in unlawful influence.

b) FORGERY OF MONEY, PUBLIC CREDIT CARDS, REVENUE STAMPS AND IDENTIFICATION INSTRUMENTS OR SIGNS (ARTICLE *25-BIS*):

1) counterfeiting of currency, spending and introduction into the State, in concert, of counterfeit currency;

2) alteration of coins;

3) spending and introduction into the State, without concert, of counterfeit money;

4) spending of counterfeit money received in good faith;

5) forgery of revenue stamps, introduction into the State, purchase, possession or putting into circulation of forged revenue stamps;

6) counterfeiting watermarked paper in use for the manufacture of public credit cards or stamps;

7) manufacture or possession of watermarks or instruments intended for the counterfeiting of currency, revenue stamps or watermarked paper;

8) use of counterfeit or altered stamps;

9) counterfeiting, alteration or use of trade marks or distinctive signs or of patents, models and designs;

10) introduction into the State and trade in products with false signs.

c) CORPORATE OFFENCES (ARTICLE *25-TER*):

1) false corporate communications;

2) false corporate communications by listed companies;

3) false corporate communications of a minor nature;

4) false prospectus[7];

5) impeded control[8] ;

6) fictitious capital formation;

7) undue return of contributions;

8) illegal distribution of profits and reserves;

9) unlawful transactions involving the shares or quotas of the company or the parent company;

10) transactions to the detriment of creditors;

---

[7] Article 34 of Law No. 262 of 28 December 2005 (laying down provisions for the protection of savings and the regulation of financial markets and also known as the 'Law on Savings') included the offence of false prospectus in the list of offences provided for by Legislative Decree No. 58/98 (Consolidated Law on Finance), in detail in Article *173-bis*, repealing, at the same time, Article 2623 of the Civil Code.

The consequence of the aforesaid repeal would seem to coincide with the removal of the offence of false prospectus from the list of so-called predicate offences and, therefore, with the consequent disappearance of the entity's administrative liability.

This would seem to be the thesis accepted by the majority doctrine; however, we consider it appropriate to give relevance to this offence, on the assumption of the orientation, albeit a minority one, which considers that, notwithstanding the transposition of the case into the Consolidated Law on Finance, false accounting continues to be relevant for the purposes of the liability of the entity.

[8] Article 37, paragraph 35 of Legislative Decree No. 39 of 27 January 2010 amended Article 2625, paragraph 1, of the Civil Code by excluding auditing from the list of activities whose obstruction by directors is sanctioned by the rule; obstruction by auditors is now governed by Article 29 of Legislative Decree No. 39/2010, which provides that '1. Legislative Decree 39/2010, which provides that "1. Members of the board of directors who, by concealing documents or using other suitable devices, prevent or in any case obstruct the performance of statutory auditing activities shall be punished with a fine of up to EUR 75,000. If the conduct referred to in paragraph 1 has caused damage to shareholders or third parties, the penalty shall be a fine of up to EUR 75,000 and imprisonment of up to 18 months, 3. In the case of statutory audits of public interest entities, the penalties referred to in paragraphs 1 and 2 shall be doubled. 4. Proceedings shall be brought ex officio.

11) undue distribution of corporate assets by the liquidators;

12) unlawful influence on the assembly;

13) agiotage;

14) obstructing the exercise of the functions of public supervisory authorities;

15) failure to disclose a conflict of interest;

16) corruption between private individuals;

17) incitement to bribery between private individuals;

18) false or omitted statements for the issue of the preliminary certificate.

With regard to the offence of falsity in the reports or communications of auditing firms, it should be noted that Article 37, paragraph 34 of Legislative Decree No. 39 of 27 January 2010 repealed Article 2624 of the Civil Code (falsity in the reports or communications of auditing firms). At the same time, Legislative Decree No. 39 of 27 January 2010 introduced Article 27, which provides for the offence of "falsity in the reports or communications of the persons responsible for carrying out the statutory audit"; the new offence is broader in application than the previous one, as it also regulates the offence committed by the auditor of a public interest entity. However, in accordance with what was established by the United Sections of the Criminal Court of Cassation in ruling No. 34476/2011, the offence of falsity in the reports or communications of the persons responsible for the statutory audit does not fall within the scope of the offences set forth in Legislative Decree No. 231/01, since the latter expressly refers to Article 2624 of the Italian Civil Code, which has been formally repealed. Therefore, in compliance with the principle of legality established by the same Article 2 of Legislative Decree 231/01, since Article *25-ter* of the DECREE has not been amended in the express reference to Article 2624 of the Civil Code, on the basis of the Court's decision, it must be considered that the offence of false statements in the reports or communications of the persons responsible for the statutory audit does not exist under the administrative liability of companies.

d) OFFENCES FOR THE PURPOSE OF TERRORISM AND SUBVERSION OF THE DEMOCRATIC ORDER (ARTICLE *25-QUATER*)

e) FEMALE GENITAL MUTILATION PRACTICES (ART. *25C*.1)

f) OFFENCES AGAINST THE INDIVIDUAL (ARTICLE *25-QUINQUIES*):

1) reduction or maintenance in slavery or servitude;
2) child prostitution;
3) child pornography;
4) possession of or access to pornographic material;
5) virtual pornography;
6) tourist initiatives aimed at the exploitation of child prostitution;
7) trafficking in persons;
8) purchase and alienation of slaves;
9) illicit brokering and exploitation of labour;
10) solicitation of minors.

g) OFFENCES OF ABUSE OF OR UNLAWFUL COMMUNICATION OF INSIDE INFORMATION AND MARKET MANIPULATION (ARTICLE *25-SEXIES*):

1) Misuse or unlawful disclosure of inside information. Recommending or inducing others to commit insider dealing;

h) Market manipulation.CULPABLE HOMICIDE AND GRIEVOUS OR VERY GRIEVOUS BODILY HARM, COMMITTED IN BREACH OF THE RULES

ON ACCIDENT PREVENTION AND HEALTH AND SAFETY AT WORK (ARTICLE *25-SEPTIES*)

i) RECEIVING STOLEN GOODS, MONEY LAUNDERING, USE OF MONEY, GOODS OR BENEFITS OF UNLAWFUL ORIGIN, AND SELFLAUNDERING (ARTICLE *25-OCTIES*)[9]

j) OFFENCES RELATING TO NON-CASH PAYMENT INSTRUMENTS AND FRAUDULENT TRANSFER OF VALUES (ARTICLE *25-OCTIES*.1):

1) misuse and falsification of non-cash payment instruments;

2) possession and distribution of computer equipment, devices or programmes intended to commit offences involving non-cash payment instruments;

3) computer fraud aggravated by the carrying out of a transfer of money, monetary value or virtual currency;

4) fraudulent transfer of valuables.

as well as any other offence against public faith, against property or otherwise offending against property provided for in the Criminal Code, when it relates to non-cash means of payment.

k) TRANSNATIONAL CRIMES (LAW 146/2006, ARTICLE 10):

1) criminal conspiracy;

[9] Legislative Decree 195/2021, implementing Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by means of criminal law, for the offences referred to in Articles 648, 648-bis, 648-ter and 648-ter1 of the Criminal Code has extended the predicate offences of the aforementioned crimes also to culpable offences and contraventions punishable by imprisonment of more than one year in the maximum or six months in the minimum.

2) mafia-type association;

3) criminal conspiracy to smuggle foreign tobacco products;

4) association for the purpose of illicit trafficking in narcotic drugs or psychotropic substances;

5) provisions against illegal immigration;

6) inducement not to make statements or to make false statements to the judicial authorities;

7) personal aiding and abetting.

It should be noted that the commission of so-called 'transnational' offences is only relevant if the offence is punishable by imprisonment of no less than a maximum of four years and an organised criminal group is involved, as well as:

- is committed in more than one State;
- or is committed in one State, but a substantial part of its preparation, planning, direction or control takes place in another State;
- or it is committed in one state, but an organised criminal group is involved in it, engaged in criminal activities in more than one state;
- or is committed in one State but has substantial effects in another State.

l) COMPUTER CRIMES AND UNLAWFUL DATA PROCESSING (ARTICLE *24-BIS*):

1) unauthorised access to a computer or telecommunications system;

2) possession, dissemination, and unlawful installation of equipment, codes, and other means designed to access computer or telecommunications systems;

3) unlawful interception, obstruction or interruption of computer or telematic communications;

4) Unlawful possession, dissemination and installation of equipment and other means of intercepting, impeding or interrupting computer or telematic communications;

5) Extortion;

6) damage to information, data and computer programmes;

7) damage to information, data and computer programmes of public utility;

8) damage to computer and telecommunications systems;

9) possession, dissemination, and unlawful installation of computer equipment, devices, or programs intended to damage or interrupt a computer or telecommunications system

10) damage to computer or telematic systems of public interest;

11) forgery of computer documents;

12) computer fraud of the entity providing electronic signature certification services;

13) failure to disclose or untrue disclosure of information, data, facts relevant to the national cybersecurity perimeter.

m) COPYRIGHT INFRINGEMENT OFFENCES (ARTICLE *25-NOVIES*):

1) offences in violation of the law protecting copyright and other rights related to its exercise.

n) OFFENCES AGAINST INDUSTRY AND TRADE (ARTICLE *25-BIS*.1):

1) disturbing the freedom of industry and trade;

2) unlawful competition with threats or violence;

3) fraud against national industries;

4) fraud in the exercise of trade;

5) sale of non-genuine foodstuffs as genuine;

6) sale of industrial products with false signs;

7) manufacture of and trade in goods made by usurping industrial property rights;

8) counterfeiting of geographical indications or designations of origin for agri-food products.

o) ORGANISED CRIME OFFENCES (ARTICLE *24-TER*):

1) criminal conspiracy (also aimed at reducing to or keeping in slavery, trafficking in persons, trafficking in organs taken from living persons, the purchase and sale of slaves and offences concerning violations of the provisions on illegal immigration and on the removal and transplantation of organs and tissues);

2) mafia-type associations, including foreign ones;

3) political-mafia electoral exchange;

4) kidnapping for the purpose of extortion;

5) criminal conspiracy aimed at the illegal trafficking of narcotic or psychotropic substances;

6) Illegal manufacture of and trafficking in weapons of war or warlike weapons or parts thereof, explosives, clandestine weapons, and common firearms.

p) OFFENCES AGAINST THE ADMINISTRATION OF JUSTICE (ARTICLE *25-DECIES*):

1) inducement not to make statements or to make false statements to the judicial authorities.

q) ENVIRONMENTAL OFFENCES (ARTICLE *25-UNDECIES*):

1) killing or possession of specimens of protected wild animal or plant species;

2) damage to habitats within a protected site;

3) environmental pollution;

4) environmental disaster;

5) culpable offences against the environment;

6) trafficking and abandonment of highly radioactive material;

7) aggravating circumstances (offences of criminal association, including mafia-type and foreign environmental offences);

8) unlawful discharges of waste water;

9) unauthorised waste management activities;

10) site remediation violations;

11) reporting violations, compulsory record keeping and environmental forms;

12) illicit waste trafficking;

13) organised activities for the illegal trafficking of waste;

14) emission and air quality limit values exceeded;

15) violations concerning the import, export and trade of protected animal and plant species;

16) violations of measures to protect stratospheric ozone and the environment;

17) malicious or culpable pollution caused by vessels.

r) CRIMES RELATING TO IMMIGRATION AND THE STATUS OF FOREIGNERS (ART. *25-DUODECIES*):

1) employment of illegally staying third-country nationals;

2) procuring unlawful entry and aiding and abetting illegal immigration.

s) RACISM AND XENOPHOBIA OFFENCES (ARTICLE *25-TERDECIES*):

1) propaganda and incitement to commit racial, ethnic and religious discrimination.

t) OFFENCES OF FRAUD IN SPORTING COMPETITIONS, UNLAWFUL GAMING OR BETTING AND GAMBLING BY MEANS OF PROHIBITED DEVICES (ARTICLE *25-QUATERDECIES*):

1) fraud in sporting competitions;

u) abusive exercise of gambling or betting activities.TAX OFFENCES (ART. *25-QUINQUIESDECIES*):

1) fraudulent declaration using invoices or other documents for non-existent transactions;

2) fraudulent declaration by means of other artifices;

3) false declaration in the context of cross-border fraudulent schemes, connected to the territory of at least one other Member State of the European Union, and in order to evade value added tax for a total amount of not less than ten million euro;

4) omitted declaration within the framework of cross-border fraudulent schemes connected to the territory of at least one other Member State of the European Union, and in order to evade value added tax for a total amount of not less than ten million euro;

5) issuing invoices or other documents for non-existent transactions;

6) concealment or destruction of accounting documents;

7) undue compensation in cross-border fraudulent schemes connected to the territory of at least one other Member State of the European Union,and for

the purpose of evading value added tax for a total amount of not less than ten million euro;

8) fraudulent evasion of taxes.

v) SMUGGLING (ART. 25-SEXIESDECIES)[10] :

;

1) smuggling due to failure to declare.

2) Smuggling by false declaration

3) smuggling in the movement of goods by sea, air and across border lakes

4) smuggling for the improper use of imported goods with total or partial reduction of duties

5) smuggling in the export of goods eligible for duty refunds

6) smuggling in temporary exportation and in special use and processing regimes

7) smuggling of manufactured tobacco

8) aggravating circumstances of the crime of smuggling manufactured tobacco

9) criminal association for the purpose of smuggling manufactured tobacco

10) equating attempted crime with actual crime

11) aggravating circumstances of smuggling

[10] For the offences indicated at Nos. 1) to 12), the violations constitute an offence (therefore also under Legislative Decree 231/01) when the amount of the border duties due exceeds €10,000 or if one of the circumstance applies pursuant to Art. 88, paragraph 1, lett from a) to d) All I D. Lgs 26 Setepermber 2024, No. 141, pursuant to Art. 96, para. 1, All I Legislative Decree of 26 September 2024 No. 141

12) repeated smuggling

13) evasion of assessment or payment of excise duty on energy products

14) evasion of assessment or payment of excise duty on manufactured tobacco

15) aggravating circumstances of the crime of evading the assessment or payment of excise duty on tobacco

16) extenuating circumstances

17) sale of manufactured tobacco without authorisation or purchase from persons not authorised to sell

18) illegal production of alcohol and alcoholic beverages

19) association for the purpose of clandestine manufacture of alcohol and alcoholic beverages

20) evasion of assessment and payment of excise duty on alcohol and alcoholic beverages

21) aggravating circumstances

22) alteration of devices, marks and labels

23) shortages and surpluses in the storage and circulation of products subject to excise duty

24) irregularities in circulation

w) OFFENCES AGAINST THE CULTURAL HERITAGE (ARTICLE *25-SEPTIESDECIES*):

1) Theft of cultural property;

2) Misappropriation of cultural property;

3) Receiving cultural goods;

4) Forgery of a private contract relating to cultural goods;

5) Violations concerning the alienation of cultural goods;

6) Illegal importation of cultural goods;

7) Illicit export or export of cultural goods;

8) Destruction, dispersal, deterioration, defacement, defacement and unlawful use of cultural or landscape assets;

9) Counterfeiting of works of art.

x) LAUNDERING OF CULTURAL GOODS AND DEVASTATION AND LOOTING OF CULTURAL AND LANDSCAPE ASSETS (ARTICLE 25-*DUODEVICIES):*

1) Recycling of cultural goods;

2) Devastation and looting of cultural and landscape assets..

y) CRIMES AGAINST ANIMAILS

1) Slaughter of animals
2) Animal abuse
3) prohibited shows or events
4) prohibition of animal fighting
5) killing or harming other people's animals

z) NON COMPLIANCE WITH PROHIBITORY SANCTIONS (ART. 23)

Chapter II

THE ITALFARMACO S.P.A. MODEL

GENERAL PART

1. ITALFARMACO

ITALFARMACO S.P.A., the parent company of the homonymous ITALFARMACO GROUP, is active in the pharmaceutical and chemical-pharmaceutical sector through the companies that it directly controls or owns shares in.

The GROUP operates both in Italy and abroad, in the research, production and sale of drugs in the cardiovascular, osteoporosis, immuno-oncological, gynaecological, neurological, thrombosis, and critical ischemia fields.

In particular, it is distinguished by its commitment to research, primarily oriented towards the cardiovascular, immunological and oncological sectors, with the objective of creating increasingly effective and safe drugs, so as to improve the health of patients and ensure that they have a better quality of life.

It has modern and sophisticated industrial plants at which, according to the highest quality standards, it manufactures proprietary medicinal products and active ingredients for the pharmaceutical sector.

The COMPANY has obtained certificates that guarantee the safety and quality of its business processes, in particular:

- quality management system certification;
- attestation of conformity with the requirements provided for in the Farmindustria reference document (ed. 2015) for the certification of procedures relating to scientific reporting activities;
- The BS OHSAS 18001:2007 quality certificate.

2. Nature and sources of the MODEL

This Organisation, Management and Control Model is an internal COMPANY regulation: it consists of the collection of operating rules and ethical rules adopted in order to prevent the commission of OFFENCES.

The MODEL is based on the *Guidelines* of the trade associations[11] for the adoption of organisational models regarding the administrative liability of organisations.

The rules contained therein are based on the results of risk mapping.

The COMPANY'S CODE OF ETHICS is the essential foundation of the MODEL, to which it is appended.

The CODE contains a number of legal obligations and moral duties for all of the organisation's participants and constitutes an effective tool for the prevention of offences.

The principles of the CODE OF ETHICS are immediately applicable to relationships between the business and institutional counterparties, including the Public Administration.

The ORGANISATION MODEL supplements the provisions of the CODE OF ETHICS.

3. Purpose

With its adoption of the MODEL the COMPANY intends to:

- comply with legal provisions, the fundamental principles of the DECREE, and the Self-Governance Codes issued by trade associations;
- make the system of controls and corporate governance more effective, with the objective of preventing the commission of OFFENCES.

The MODEL establishes the following objectives:

- to inform the RECIPIENTS about the activities that pose the risk of the commission of OFFENCES, the procedures to be followed in the carrying out of activities exposed to risk, the penalising consequences of breaches of legal provisions, and the COMPANY'S internal rules;
- to maintain a business culture inspired by lawfulness;

[11] In particular, the *Guidelines* developed by FARMINDUSTRIA.

- to establish a culture of control, which must preside over the achievement of the COMPANY'S objectives;
- to establish the principles of an efficient and balanced organisation, with particular regard to the allocation of powers, decision-making, control of activities, and internal and external reporting.

Taking into account the nature and size of the organisation, as well as the type of activity or function performed, it must adopt measures specifically aimed at the following:

- ensuring compliance with the law and internal rules;
- the timely elimination, or at least minimisation, of situations subject to the risk of the commission of offences.

For the purposes outlined in the previous paragraph, the COMPANY adopts and implements regulatory, organisational and procedural rules for:

- ensuring that staff members are hired, managed and trained in compliance with the CODE OF ETHICS, the MODEL, and legal provisions;
- encouraging the implementation of the Model by all individuals operating within the COMPANY;
- guaranteeing the protection and confidentiality of those who provide information on non-compliant conduct;
- guaranteeing that the distribution of powers, competences, functions, tasks and responsibilities among the individuals operating within the COMPANY, as well as their placement within the business organisation, is in line with the principles of transparency, clarity, verifiability and consistency with the activity carried out specifically by the COMPANY;
- penalising conduct that does not respect the limits of the duties and powers established by the law and internal documents;
- ensuring that the determination of the COMPANY'S objectives, as well as those established for the RECIPIENTS, meet realistic criteria of objective practicability;
- describing the business organisation, functional structure, activities carried out by the COMPANY and relations with other companies in the GROUP or other

organisations, in accurate and correct documents, updated in a timely manner by identified individuals;

- implementing training and continuous development programmes in order to ensure that the CODE OF ETHICS and the MODEL are effectively known by those who operate within the COMPANY, as well as the individual involved in the activities exposed to risk and operations over which ITALFARMACO exercises managerial and controlling power;
- allowing the use of IT tools and internet access exclusively for purposes linked to the employee's working activity, in accordance with company regulations.

4. Recipients

The rules contained in the MODEL apply to:

- anyone who, including on a de facto basis, performs functions pertaining to the representation, management, administration, direction or control of the COMPANY, or a unit or division with financial and functional autonomy (COMPANY REPRESENTATIVES);
- the COMPANY'S subordinate employees under any kind of contractual relationship, even if they are stationed abroad (EMPLOYEES);
- anyone operating on a contract basis or in the interests of the COMPANY;
- COLLABORATORS and THIRD PARTIES under contractual regimes that permit the exercise of managerial and controlling authority by ITALFARMACO.

The MODEL and the CODE OF ETHICS constitute a point of reference for the suppliers of goods and services, consultants, partners in temporary associations and companies with which ITALFARMACO operates.

Agreements between members or partners must include acceptance of the rules contained in those documents.

The RECIPIENTS are obliged to fully comply with all of the provisions of the Model, also in accordance with the duties of loyalty, fairness and diligence that emerge from the legal relationships established with the COMPANY.

ITALFARMACO condemns and sanctions any conduct that contradicts or eludes legal provisions, the MODEL or the CODE OF ETHICS, even if the conduct is carried out in the conviction that the COMPANY'S interests are being pursued or that it will be advantageous to the COMPANY.

5. Communication and training on the MODEL

The COMPANY sends the MODEL and the CODE OF ETHICS to all RECIPIENTS by means of processes that can ensure that RECIPIENTS effectively gain knowledge of said Model and CODE OF ETHICS.

They are sent to new employees upon appointment and to collaborators upon the signing of the contract.

Adoption of the Model is communicated to third parties (promotors, agents, collaborators under so-called "*para-subordinate*" contracts, consultants, outsourcers, suppliers, business partners) and differentiated methods of publicity are provided for depending on the type of contractual relationship and activity carried out in relation to the risk of offences being committed.

The COMPANY organises periodic training activity, differentiated according to the various types of RECIPIENT and the sensitive areas in which they operate.

In particular, the training is provided for new recruits and, in the event of changes or updates to the MODEL, all RECIPIENTS.

The training is managed by the competent function, which coordinates with the COMPLIANCE COMMITTEE and the managers of the functions involved at any given time.

6. Adoption, amendment and updating of the MODEL and PROCEDURES.

The BOARD OF DIRECTORS has exclusive responsibility for the updating and revision of the MODEL:

- it provides for amendments if significant violations or elusions of the requirements demonstrating that the MODEL is inadequate are identified (by the COMMITTEE, another of the COMPANY'S functions, or any other individual);

- it updates the MODEL in a timely manner, including at the proposal of the COMMITTEE, if there are changes or amendments:
    a. to the legislative and regulatory system governing the COMPANY'S activity;
    b. to the corporate structure, internal organisation or structure;
    c. to the COMPANY'S activity, or the goods or services offered to clientele;
    d. in relation to the mapping of risks.

The functional structures involved draw up amendments to the procedures for which they are responsible in a timely manner, as necessary for the effective updating of the MODEL.

The proposed amendments are reported in advance to the COMMITTEE, which expresses an opinion in a timely manner. If the BOARD OF DIRECTors decides to deviate from them, it must provide adequate justification.

Each of the COMPANY'S Managing Directors can make formal changes to the MODEL and procedures as necessary to ensure greater clarity and efficiency. The changes are immediately reported to the COMMITTEE and the Managing Director for ratification.

The Committee must promptly inform the Chairman of the BOARD OF DIRECTORS and the Managing Directors in writing of the appropriateness or necessity of amending or revising the MODEL. In such cases, the Chairman of the BOARD OF DIRECTORS must convene a Board Meeting in order for resolutions that fall within its scope of competence to be adopted.

To the extent that they are compatible, these provisions apply to the adoption of new procedures and the amendment of existing procedures, as necessary for the implementation of the MODEL. The introduction and revision of procedures is communicated to the COMMITTEE in a timely manner.

7. Provision of intra-group services

7.1. Provision of services to subsidiaries

The provision of services to subsidiaries in the context of activities exposed to risk must be governed by a written contract, which must be communicated to the COMPLIANCE COMMITTEE.

In particular, the contract must provide for:

- the obligation for the beneficiary company to attest to the accuracy and completeness of the documentation and information communicated to the COMPANY, for the purposes of the provision of the required services;
- the COMMITTEE'S power to request information from the beneficiary company's Compliance Committee or equivalent function;
- the obligation for the COMMITTEE to draw up a report on the functions carried out in relation to the required services at least once a year. The report is communicated to the BOARD OF DIRECTORS and Compliance Committee of the beneficiary company;
- the beneficiary company's Committee having the power to request information from ITALFARMACO'S COMMITTEE, or the competent functions, subject said body or function being informed.

In the provision of services, the COMPANY complies with the CODE OF ETHICS, the MODEL and the procedures established for its implementation.

If the COMPANY provides services on behalf of other GROUP companies in the context of activities exposed to risk or operations not considered in the MODEL itself, it establishes adequate rules and procedures to prevent the commission of OFFENCES.

If the beneficiary company justifiably requires compliance with new procedures or procedures that differ from those provided for by this MODEL or established for its implementation, the COMPANY will only follow such procedures after the COMMITTEE has deemed them suitable for the prevention of offences.

The COMPLIANCE COMMITTEE is responsible for the adoption of and compliance with the procedures.

7.2. Provision of services by subsidiaries to the COMPANY

Services provided by subsidiaries to Italfarmaco which involve the carrying out of activities exposed to risk must be governed by a written contract, which must be communicated to the COMPLIANCE COMMITTEE.

The contract must provide for:

- the OBLIGATION for the COMPANY to attest to the accuracy and completeness of the documentation and information provided for the purposes of the provision of the required services;
- ITALFARMACO'S COMMITTEE having the power to request the Compliance Committee of the company providing the services, or its competent functions, for information, subject to the COMMITTEE being informed;
- the duty for the COMMITTEE to draw up a report on the performance of its own functions at least once a year, and to communicate it to the ITALFARMACO'S BOARD OF DIRECTORS and COMMITTEE.

The contracts must stipulate that the subsidiary must have a MODEL or, in any case, suitable procedures for preventing the commission of OFFENCES.

If the adoption of the MODEL is not required by the legislation governing the activity of the GROUP company, COMPANY must, after consulting its own COMMITTEE, verify whether the subsidiary's organisational structure and internal procedures are suitable for preventing the commission of offences.

The COMPANY may justifiably request compliance with new procedures or procedures that differ from those provided for by its Model. The company providing the services must follow those procedures only after its own Committee has deemed them suitable for preventing the commission of offences.

After consulting the competent functions, the COMMITTEE may propose that the contracts provide for the adoption of specific control procedures by the company.

8. Identification of the COMPLIANCE COMMITTEE

The DECREE requires the following tasks to be entrusted to a "*body within the organisation*" with "*autonomy and powers of initiative and control*":

- continuously monitoring the functioning, compliance and effective implementation of the MODEL by employees, corporate bodies, service companies and third parties;
- ensuring the timely and constant updating of the MODEL in relation to changing business and regulatory conditions.

The COMMITTEE must be characterised by: stability, budgetary and hierarchical autonomy in relation to the other bodies and individuals within the COMPANY, independence of judgment and interests, as well as professionalism, operational efficiency and continuity of action.

The requirements of *autonomy and independence* presuppose that the COMMITTEE:

- possesses autonomous powers of initiative and control;
- answers only to the highest hierarchical position, namely the BOARD OF DIRECTORS;
- does not operate on a subordinate basis or on the basis of the directives of any other function, senior management or the decision-making body;
- does not take on operational responsibilities.

In the performance of its functions, the COMMITTEE shall encourage rational and efficient cooperation with the COMPANY'S bodies and control functions.

The requirement of professionalism presupposes that the COMMITTEE:

- possesses adequate specialist competencies, particularly with regard to financial offences;
- is equipped with specialist tools and techniques in order to be able to perform its activities, making use of specialist internal and external assistants.

The requirement of honour presupposes the absence of reasons for ineligibility: for members of the COMMITTEE, they must not have been subject to rulings of conviction, even in the first instance, or plea deals, relating to offences that render the organisation liable; they must not be subject to any reason for ineligibility provided for banking representatives and financial intermediaries.

The COMMITTEE is composed of three members, at least two of whom have specific professional expertise in matters relevant to the COMPANY (external members) and one

member with specific knowledge of the COMPANY, who may also belong to the COMPANY 's staff (external member with specific knowledge of the COMPANY, or internal member). Specifically, the COMMITTEE is made up of one member belonging to the COMPANY'S staff, identified as the Manager of the Regulatory Affairs and Compliance Function, and two external members.

The COMMITTEE appoints a Secretary from among its members, to whom the filing and storage of the documents concerning the COMMITTEE'S activity is entrusted. The Secretary is responsible for ensuring that the documentation cannot be modified or altered.

The BOARD OF DIRECTORS is responsible for appointing and removing the members and Chairman of the COMMITTEE, subject to the opinion of the Statutory Auditors, with a justified order for each member. Specific functions can be delegated to the Chairman, chosen from among the external members.

The removal of each member can be ordered in a joint session with the board of statutory auditors, in which other members of the COMMITTEE also participate.

In choosing members, the only relevant criteria are:

- the specific professionalism and competence required for the performance of the functions;
- honour,;
- for the external members, absolute independence from the COMPANY.

The same requirements are valid for external consultants.

The appointment decision defines the duration of the appointment and the cases of revocation.

The appointment is for a period of preferably three years and is renewable.

Revocation is permitted in the following cases:

- for just cause (for example, disloyalty, inefficiency, negligence, lack of expertise, breaches of confidentiality obligations, gross breaches of the duties defined in the MODEL);
- supervening impossibility;

should the members of the COMMITTEE no longer meet the requirements of independence, impartiality, autonomy, honour and eligibility, as well as the absence

of conflicts of interest and family relationships with members of the corporate bodies or senior management;

- when the relationship of employment or collaboration with the COMPANY ceases.

Every member of the COMMITTEE must inform the Secretary and the other members if they cease to meet requirements.

The COMMITTEE is understood to be dissolved in the following cases:

- if the majority of its members leave, due to resignation or other causes;
- if, in relation to the COMPANY, a judgment of conviction or plea deal is handed down for violations of the DECREE, and the inadequacy or omission of the supervisory activity is established.

The COMMITTEE governs its own functioning with a specific regulation.

9. Function and powers of the Committee

The Committee is responsible for supervisory functions:

a) concerning the *effectiveness* and adequacy of the MODEL in order to prevent the commission of offences.

   To this end, according to the frequency deemed appropriate, the COMMITTEE:

   - interprets the relevant legislation;
   - conducts inspections of company activity in order to update the mapping of activities exposed to risk and the related sensitive processes;
   - coordinates with the function responsible for defining and implementing staff training and development programmes;
   - monitors initiatives for raising awareness of the MODEL within and outside of the Company;

b) concerning *compliance* with the MODEL by the corporate bodies, staff and third parties.:

To that end, the COMMITTEE:

- periodically carries out checks aimed at identifying sensitive operations, with or without advance notice;
- coordinates with business functions to monitor activity. The COMMITTEE has free access to company documentation and is constantly informed of: the activities that may expose the COMPANY to the risk of the commission of OFFENCES; relations with service companies and third parties operating on behalf of the COMPANY in the context of sensitive operations; extraordinary activities;
- gathers, processes and stores relevant information for compliance with the MODEL;
- updates the list of information to be sent or made available to the COMMITTEE;
- arranges internal inquiries, coordinating with the business functions involved, to acquire further evidence for assessment;

c) concerning the *need* to update the MODEL in the event of changes to business and regulatory conditions.

To that end, the COMMITTEE:

- sends a periodic assessment of the MODEL'S adequacy to the BOARD OF DIRECTORS;
- periodically checks the implementation and effective functionality of proposed corrective actions, at least every six months;
- coordinates with the managers of the competent business functions in order to assess the adoption of any disciplinary penalties.

In the context of its supervisory activity, the COMMITTEE has the following powers of initiative and control, which it exercises in compliance with the law and the rights of the interested parties:

- it carries out periodic inspections and checks, including on a sample-basis, and possibly coordinating with the organisation's Compliance functions; it establishes their frequency in relation to the areas of intervention and types of sensitive activity;

- it has access to all information concerning activities exposed to risk;
- it can, with or without advance warning, request information from all individuals internal and external to the COMPANY who are obliged to comply with the MODEL or ask to be shown documents, including electronic documents, concerning activities exposed to risk. The obligation for external parties to comply with the COMMITTEE'S requests must be included in the contracts governing their relations with the COMPANY;
- it may request information or documents about subsidiaries or companies in which the Company owns shares, through a request addressed to the individual company's Compliance Committee or equivalent body;
- it periodically receives, according to a pre-determined schedule, reports and information from the managers of the functional areas involved in activities exposed to risk;
- it can make use of personnel belonging to business functions for its verification activities. To that end, it can identify a dedicated team and coordinate the use of personnel with the manager of the function in question;
- it receives annual work plans from the internal functions that carry out auditing and compliance activities, with specific details on the areas exposed to risk. The COMMITTEE may send a justified request for the plans to be supplemented, informing the Board of Directors and the Board of Statutory Auditors;
- it may make use of external consultants, informing the Managing Director. This communication may be omitted due to the particular delicacy of investigations, or the subject thereof;
- it reports any need to commence penalty procedures to the Managing Director;
- it informs the Managing Director of breaches of measures aimed at protecting whistleblowers, as well as unfounded reports and reports submitted in wilful misconduct or gross negligence;
- it subjects the MODEL and the procedures adopted for its material implementation to periodic checks, at least every six months, and proposes any updates to the decision-making Body;

- it sends the Chairman of the BOARD OF DIRECTORS and the Chairman of the Board of Statutory Auditors a written report on the activity carried out and a justified account of its expenses, every six months or more frequently if required due to the critical nature of the issue at hand. The reports, included in the minutes book, contain any proposals to supplement or amend the Model and the procedures;
- it can request meetings with the Board of Statutory Auditors, the BOARD OF DIRECTORS or the Managing Director. In turn, the latter may request a direct meeting with the COMMITTEE;
- it prepares an annual plan of the following year's activity, to be submitted to the BOARD OF DIRECTORS at its next meeting, and to the BOARD OF DIRECTORS. Weekly reports on the activities carried out by the COMMITTEE and the relative outcomes are drawn up and sent to the BOARD OF DIRECTORS;
- it prepares budget forecasts within ninety days of the end of the company's financial year;
- it coordinates with the Managing Director and the Manager of the HR Department in order to define training programmes, distribution channels and the contents of periodic communications.

In short, the periodic reports prepared by the COMMITTEE must contain:

- an account of any critical aspects concerning the means of implementing the MODEL and the CODE OF ETHICS;
- an account of the reports received with regard to the implementation of the MODEL and the PROCEDURES, without breaching anonymity or whistleblower protection obligations;
- the disciplinary procedures and any penalties applied by the COMPANY'S functions;
- a comprehensive assessment of the implementation and effectiveness of the MODEL, with any indications for its amendment, paying particular attention to the systems for managing financial resources that are able to identify atypical cash flows;
- an account of changes to the MODEL and employee awareness-raising activities.

The periodic communications to be addressed to the COMPLIANCE COMMITTEE are specified in the "*Information Flows*" document appended to this MODEL.

The COMMITTEE is supported by the Compliance function in its supervisory and control activities. It may also make use of support from other internal structures and functions, in accordance with the rules and principles set out in the internal regulations, in addition to external consultants.

The COMMITTEE has autonomous spending powers on the basis of an annual budget approved by the BOARD OF DIRECTORS.

Moreover, it may use resources that exceed its spending powers, as necessary to address any exceptional and urgent situations. The COMMITTEE must inform the BOARD OF DIRECTORS thereof at its next meeting.

The COMMITTEE cannot be given powers to intervene in managerial, decision-making, organisational or disciplinary matters.

The COMMITTEE'S control and verification activity cannot replace the COMPANY'S control functions.

Members of the COMMITTEE and the individuals that it uses to support it are obliged to keep confidentiality over all of the information obtained in the exercise of their functions.

The COMMITTEE meets at least every quarter and keeps the minutes of its meetings, under the responsibility of the Secretary.

Meetings with the COMPANY'S other bodies must be documented. A copy of the meetings is held both by the COMMITTEE and by the other bodies involved.

10. Obligations to report information to the Compliance Committee

In order to facilitate the supervisory activity on the effectiveness and functioning of the MODEL, the COMMITTEE is entrusted with:

- information useful and necessary for the performance of the supervisory tasks entrusted to the COMMITTEE itself;
- reports of alleged or actual violations of the Model and/or unlawful conduct relevant pursuant to Legislative Decree 231/2001, occurring or in progress.

Information

Within the company, the function managers of COMPANY must inform the COMMITTEE:

- at the request of the Supervisory Body and in accordance with the procedures defined by it, the information and control activities carried out, at the level of its own operational area, useful for the performance of the Supervisory Body's activities in terms of verifying compliance with, effectiveness and updating of this MODEL and from which facts, acts, events or omissions with critical profiles may emerge with respect to compliance with the provisions of Legislative Decree No. 231/2001;
- on a regular basis, the information identified in this MODEL, as well as any other information identified by the Body and requested by IT to the individual organisational and managerial structures of COMPANY through internal directives. Such information must be transmitted at the times and in the ways to be defined by the Body;
- any other information also coming from third parties and pertaining to the implementation of the MODEL in the 'sensitive' areas of activity and to compliance with the provisions of the DECREE, which may be deemed useful for the performance of the tasks of the COMMITTEE. In particular, by way of example but not limited to, information concerning the following must be mandatorily and promptly forwarded to the Body:

- measures and/or information from the judicial police, financial administration or any other authority, from which it can be inferred that investigations have been carried out for the offences referred to in the Decree, even against unknown persons;
- requests for legal assistance made by managers and/or employees in the event of legal proceedings being brought against them for offences under the DECREE;
- operations on the share capital, operations for the allocation of profits and reserves, operations for the purchase and sale of shareholdings in companies or their branches, merger, demerger and spin-off operations, as well as all operations, including those within the Group, that could potentially damage the integrity of the share capital;
- decisions relating to the application for, disbursement and use of public funding, including European funding;

- information on the actual implementation, at all levels of the company, of the MODEL, WITH evidence of disciplinary proceedings carried out and any sanctions imposed or orders to dismiss such proceedings and the reasons thereof;
- the system of directors' powers and any subsequent amendments and/or additions thereto, as well as the organisational structure;
- the company signature power system and any subsequent amendments and/or additions thereto;
- reports and/or news concerning offences committed in violation of the rules on accident prevention and on the protection of hygiene and health at work;
- other documents from which facts, acts, events or omissions may emerge with critical profiles with respect to compliance with the provisions of Legislative Decree No. 231/2001.

Reports

For the purposes of reporting, conduct, acts or omissions consisting of unlawful conduct within the meaning of Legislative Decree 231/01 or violations of the MODEL ARE considered violations.

An internal report is defined as the written or oral communication of information on violations, acquired in the work context, submitted through a channel activated by the COMPANY that guarantees the confidentiality of the reporter and the person involved (natural or legal person mentioned in the report as the person to whom the violation is attributed or implicated in the report), the content of the report and the relevant documentation.

Information on violations covers information, including reasonable suspicions, concerning violations committed or which, on the basis of concrete evidence, could be committed in the organisation, as well as elements concerning conduct aimed at concealing such violations.

COMPANY provides clear information on the channel, methods and prerequisites for making internal reports through the "Whistleblowing Procedure" (Annex 3), which regulates the process of acquiring and managing reports in compliance with the provisions of Legislative Decree 24/2023 and Legislative Decree 231/01. The internal reporting procedure is displayed and made visible in the workplace and published on the COMPANY's website/intranet.

COMPANY, in accordance with the provisions of Legislative Decree 24/2023, complies with the protective measures provided for by law, including the prohibition to engage in retaliatory acts, even by way of attempt or threat.

The adoption of discriminatory measures against whistleblowers may be reported by the whistleblower to the ANAC for measures within its competence.

All processing of personal data is carried out in accordance with Regulation (EU) 2016/679, Legislative Decree No 196 of 30 June 2003 and Legislative Decree No 51 of 18 May 2018.

As provided for in the "Whistleblowing Procedure", the collegiate body responsible for the management of whistleblowing reports ("channel manager") is required to transmit to the COMMITTEE, while maintaining confidentiality obligations, any report that has potential relevance for the purposes of Legislative Decree 231/01 and the application of the MODEL.

The COMMITTEE assesses the reports received and any consequent measures and adopts any measures it deems necessary for the purposes of adapting the MODEL, giving rise to the communications necessary for the Company to apply any sanctions. Any consequent measures are applied in compliance with the provisions of the sanctions system set out in Chapter 12 below.

In addition to internal reporting, it is also possible to communicate information on violations through an external reporting channel activated by ANAC in accordance with Article 7 et seq. of Legislative Decree 24/2023 and only if the regulatory conditions are met. The procedures for submitting and managing external reports are governed by the Guidelines adopted by ANAC on 12 July 2023 and can be activated through the ANAC channels mentioned in the 'Whistleblowing Procedure'.

Reports, internal and external, and related documentation are kept for as long as necessary to process the report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure.

11. Documentation of the COMMITTEE'S activity and the gathering and storage of information

The COMMITTEE'S supervisory activities are documented.

For every intervention, it is required to:

- define a detailed plan of work for the activities provided for in the annual programme of checks;
- make written requests to the organisational units involved;
- file the documentation produced and received, including in electronic format, in chronological order; draw up a report on every intervention and the evidence that has emerged;
- update the register with activities carried out.

The following must be recorded in the register:

- training activities;
- duration of and justification for the checks, the organisational units involved, and any suggestions;
- reports received for every sensitive activity, specifying the structures involved;
- updates to the MODEL, specifying the principal amendments. The Secretary is

responsible for keeping a book of minutes of the COMMITTEE'S meetings.

All of the information and reports provided for in this MODEL are stored by the COMMITTEE on paper and in digital format for a period of ten years, without prejudice to the different data retention period provided for whistleblowing reports and detailed in the previous paragraph. Compliance with the provisions on the privacy of personal data remain without prejudice.

Only the COMMITTEE and the individuals identified in the COMMITTEE'S Regulation are allowed access to said information and reports.

12. The disciplinary system

Article 6(2) of the DECREE provides for the introduction of a disciplinary system designed for the penalisation of breaches of the MODEL and the procedures in order to render the control system effective.

The application of penalties does not prejudice or modify any consequences under civil, criminal, administrative or tax law which may derive from the offence.
The COMPANY may therefore request compensation for damages incurred as a result of breaches of the MODEL or the procedures, regardless of the imposition of penalties.
Moreover, the disciplinary procedure is implemented independently from the initiation and outcome of any criminal proceedings. In any case, the COMPANY may decide to wait for the outcome of any legal proceedings that have commenced or for the issuing of a court order, which may or may not be final, before deciding whether to start a disciplinary procedure. In such cases, temporary dismissal from service may be imposed. Every breach or evasion of the MODEL or the procedures and the penalties imposed must be reported immediately to the COMMITTEE, which monitors the compliance system.

In particular, if the COMMITTEE becomes aware of breaches of the MODEL by RECIPIENTS or contractual counterparties, it informs the Manager of the competent function and the area to which the contract or relationship relates, by means of a written report.

Moreover, the COMMITTEE submits the following to the Managing Director:

- reports relating to breaches of the MODEL and the PROCEDURES;
- violations of measures adopted to protect whistleblowers, as well as cases of unfounded reports and reports submitted in wilful misconduct or gross negligence. The adoption of the penalties provided for by the MODEL will be decided on in proportion to the importance and gravity of the offences. In the most serious cases, the disciplinary measure may consist of termination of the employment relationship or, for collaborators or third parties, their existing contract.

The BOARD OF DIRECTORS involves the functions that have disciplinary powers to decide on the application of penalties.

The procedure is carried out in accordance with the national collective bargaining agreement for the chemical-pharmaceutical sector.

The disciplinary system is differentiated for employees, managers, directors and the Board of Statutory Auditors, as well as collaborators and third parties.

For employees and managers, the penalties are applied in accordance with the provisions of the WORKERS' STATUTE and the national collective bargaining agreement in force.

After consulting the Human Resources Manager, the Legal and Corporate Affairs Manager and the COMMITTEE, as well as the managers of the functional structures involved, the BOARD OF DIRECTORS establishes the types of legal relationships with entities external to the COMPANY to which the MODEL and the penalty measures are applied.

A prerequisite for the application of penalties is that the provisions of the MODEL and the implementing procedure must be reported to persons who are obliged to comply with them by means of service orders, circulars, instructions or other appropriate methods in use at the COMPANY.

12.1. EMPLOYEES

Pursuant to Article 7(1) of Italian Law no. 300 of 20 May 1970, and Articles 38, 39 and 40 of the national collective bargaining agreement for employees in the chemical-pharmaceutical sector, the following disciplinary measures are provided for:

- *Verbal warning*

This is issued for minor breaches of the MODEL or procedures committed for the first time.

- *Written warning*

This applies for non-minor breaches of the provisions of the MODEL or procedures.

- *Fine not in excess of 4 hours of normal remuneration*

This is imposed in cases of *repeated* breaches of the procedures or the MODEL.

- *Suspension from service or from remuneration for a maximum of 8 days*

This can be imposed due to a failure to comply with the MODEL or internal procedures, and for the commission of acts that are contrary to the COMPANY'S interests and cause damage to it or expose it to situations that objectively endanger the integrity of the COMPANY'S assets.

- *Disciplinary dismissal due to notable violation of the employee's contractual obligations (justified reason or just cause)*

This is imposed in cases of conduct that does not conform to the provisions of the MODEL, aimed unequivocally at the commission of OFFENCES, causing notable damage and prejudice to the COMPANY.

In any case, if the nature of the act does not allow for the continuation of the relationship, even on a provisional basis, immediate dismissal may be imposed pursuant to Article 2119 of the Italian Civil Code, without prejudice to the implementation of disciplinary procedures.

Moreover, on appeal, the revocation of any measures imposed on the person concerned may also be ordered.

In order to establish the type and extent of each penalty, the following criteria are taken into account:

- the intentionality of the conduct or the degree of culpability, taking account of the foreseeability of the event;
- the employee's overall conduct, with particular regard to disciplinary procedures;
- the employee's functions and duties;
- other circumstances that are relevant to the assessment of the matter.

12.2. MANAGERS

The disciplinary measures for MANAGERS are as follows:

- *Warning letters*

These are provided for non-serious breaches of the MODEL or procedures.

- *Fine not in excess of 4 hours of normal remuneration*

This is imposed in cases of *repeated* breaches of the procedures or the MODEL.

- *Suspension from service or remuneration for a maximum of 8 days*

This is applied in cases of violations acts that are contrary to the COMPANY'S interests and cause damage to it or expose it to situations that objectively endanger the integrity of the COMPANY'S assets.

- *Termination of the relationship*

This may be imposed, with or without immediate effect, if clear violations of the provisions of the MODEL are committed: conduct aimed unequivocally at the commission of an OFFENCE, causing gross damage to the COMPANY. In these cases, the COMPANY'S faith in the MANAGER is radically lost.

12.3. DIRECTORS and the BOARD OF STATUTORY AUDITORS

In the event of violations of the MODEL and the procedures by directors, the COMMITTEE immediately informs the Chairman of the BOARD OF DIRECTORS and the Board of Statutory Auditors by means of a written report.
If the violation is committed by a member of the Board of Statutory Auditors, the Committee immediately informs the Chairman of the BOARD OF DIRECTORS and the Board of Statutory Auditors by means of a written report.

The penalties applicable by the BOARD OF DIRECTORS, after consulting the Board of Statutory Auditors, are as follows:

- *Warning letters*

  These are issued for non-serious breaches.

- *Fine not exceeding three times the monthly remuneration*

  This is imposed in the event of violations of intermediate gravity or repeated violations.

- *Revocation of delegated powers or removal from office*

  In the most serious cases which damage the COMPANY'S confidence, the BOARD OF DIRECTORS may convene a Shareholders' Meeting to propose removal from office.

12.4. EXTERNAL COLLABORATORS AND THIRD PARTIES

These penalties are imposed by the Managing Director, in the scope of his responsibility.

The relevant disciplinary measures, which are also specified in the contracts governing the employment relationships with the COMPANY, are as follows:

- *Warning letters*

  These are issued for non-serious violations of the MODEL.

- *Fine not exceeding one tenth of the monthly remuneration*

  This is imposed in the event of violations of intermediate gravity or repeated violations.

- *Termination of the contractual relationship*

The most serious conduct, as explicitly provided for by the so-called "clause 231" included in the letters of appointment or partnership agreements, may lead to the termination of the contractual relationship.

12.5. Cases of breaches of whistle-blower protection measures

The disciplinary system adopted pursuant to Article 6(2)(e) and (2-bis) of Legislative Decree No. 231/2001 provides for sanctions to be applied against those whom the Company ascertains to be responsible for violations of the measures for the protection of whistleblowers referred to in Section 10.

Such violations include:

- acts of retaliation;
- obstacle, even in the attempted form, to reporting;
- breach of the duty of confidentiality;
- failure to establish reporting channels;
- failure to adopt procedures for making and handling reports, or adoption of non-compliant procedures;
- failure to verify and analyse the report;
- civil liability of the reporting person for defamation or slander in cases of wilful misconduct or gross negligence, unless that person has already been convicted, also at first instance, of the offences of defamation or slander;
- Failure to transmit or late transmission of the report to the competent person if the reporting person addresses the report to a person other than the one designated to receive it.

In particular:

- against the persons held liable, the sanctions governed by the preceding paragraphs shall be applied, graduated according to the seriousness of the breach;.
- against members of the COMMITTEE, the sanction of dismissal is applicable;
- The process of ascertaining and deciding on the sanction to be applied is in the hands of the Board of Directors.

CHAPTER III

THE MODEL OF ITALFARMACO S.P.A.

SPECIAL PART

1. Background

In compliance with Article 6 of the DECREE, in relation to the offences to be prevented, the internal control system must include the following:

- specific protocols to programme the generation and implementation of the COMPANY'S decisions;
- provision for the management of appropriate financial resources to prevent the commission of offences.

The procedures that make up the prevention and control system adopted by the COMPANY are listed in the "*Organisational oversight*" document annexed to this MODEL.

The procedures must be followed by the:

- corporate bodies:
- managers;
- employees;
- Collaborators, Agents, Consultants and other counterparts, if the clauses in their contracts provide for this and allow for management and control operations on the part of the COMPANY.

The procedures are constantly updated, also upon proposal or recommendation of the COMMITTEE.

The COMMITTEE makes sure that the procedures ensure compliance with the principles contained in the MODEL. It proposes any changes and, together with the relevant corporate functions, defines the *relevant* operations to which the procedures apply.

The *relevance* markers are: the value and economic scope of the transaction with respect to the COMPANY'S area of operations; its impact on the decision-making and production processes; its relevance with respect to ordinary business operations.

In particularly urgent cases or when it is temporarily impossible to comply with the procedures, any necessary exceptions in the generation or implementation of decisions are allowed, under the responsibility of whoever puts them into effect. In that case, the COMMITTEE is immediately notified and subsequent ratification by the competent person is required.

2. General Principles

In order to prevent the commission of the OFFENCES in the areas, activities and operations exposed to risk, the COMPANY drafts and adopts procedures that must comply with the following general principles.

The COMPANY'S organisation system must be guided by compliance with laws, regulations and the integrity of the company's assets and is founded on the:

- clear, formal and comprehensible description of the tasks and powers conferred to each function, position and professional role;
- detailed description of the lines of reporting;
- traceability of each significant decision-making and operational step.

2.1. The system of proxies and powers of attorney

The following must be clearly defined and known within the organisation: the powers (and relative limits) of the persons authorised to enter into commitments and express the will of the COMPANY; the responsibilities conferred for the management of the company's business operations and processes.

The organisational and signatory powers (proxies, powers of attorney and spending limits) must be commensurate with the organisational responsibilities assigned.

The powers of attorney and proxies system is described in a constantly updated document officially approved by the Board of Directors, specifying the powers - including spending or financial powers - and the limits of autonomy. Mechanisms for publicising these vis-à-vis external stakeholders are established.

A procedure is in place for assigning proxies, establishing the:

- professional skills and requirements that the representative must possess;
- proxies and functions conferred;
- representative or substitute representative's express acceptance of the functions and assumption of the obligations thereto;
- oversight of the consistency of the proxies and substitute proxies with the activities exposed to risk and of the ongoing existence of the requirements and skills of the appointed representative;
- periodic assessment of the representative or substitute representative's technical and professional skills and the recording of those assessments;
- management of expenditure commitments.

Proxies are conferred on the basis of the principles of the representative's technical and professional eligibility and decision-making and financial autonomy, as well as the availability of adequate resources for the task and ongoing performance of the services.

The person with the proxy must have:

- decision-making powers commensurate with the proxies officially conferred;
- a budget for performance of the functions, with the possibility of going over budget for exceptional events or situations;
- a reporting obligation according to established methods for performing the functions.

2.2. Formalising and separating phases: traceability of operations

Within each relevant company process, the competence for making decisions, implementing, controlling and recording transactions must be allocated to different persons. It must be possible to trace the authorisation levels, the generation of the documents, specifying the reason, and the material and recording operations.

A Process Manager is identified and is the person in charge of the function responsible for managing the operation, unless otherwise indicated for exceptional reasons.

The Process Manager may ask for information and clarification to the functional structures, the operating units and the persons involved in performing the operation.

The recipient of the query must: forward the documentation required to respond to the request; certify the source and, where possible, the completeness and truthfulness of the information communicated or, alternatively, name the persons who can provide that certification.

The Process Manager periodically informs the COMMITTEE of all the relevant operations that fall within the scope of sensitive activities: they must provide, under their own responsibility, the information necessary to assess the risk and critical aspects of the operation.

2.3. Traceability of operations and records

The documents relating to operations subject to risk identified as relevant and sensitive in this MODEL must allow the identification of all responsible persons, in particular:

- hard copy documents must include the date on which they were written and viewed, as well as the recognisable signature of the compiler;
- the control documentation must contain the name of the person who conducted the controls, the date and the result;
- in the case of email communications, the sender and the transmission date are considered for the purposes of attribution of responsibility.

The company process managers prepare periodic reports of the activity performed. Management indicators may be used to promptly identify irregularities and anomalies.

IT systems are adopted to ensure that operations are correctly and truthfully attributed to the responsible persons: the system must ensure that records cannot be changed without leaving evidence thereof.

Every log-on to the company's IT network (intranet and internet) to perform or document operations must take place with the use of a periodically changed double asymmetric key (user ID and personal password), or, alternatively, with a procedure that allows connection to the step for which the person is responsible, leaving unalterable evidence thereof.

Hard copy and electronic documents are filed by the competent function in appropriate storage areas that protect data confidentiality and prevent damage and loss.

Specific mechanisms must be used for the protection of the data and corporate assets and the physical-logistical access thereto.

Should the document filing or storage be performed by an external person on behalf of ITALFARMACO, the service is regulated by a contract. The provider of the service must comply with procedures that prevent alteration of the data, unless amendments can be traced.

Access to the stored documents must be justified and is granted only to authorised persons and their delegates, the Board of Statutory Auditors, the independent auditors, if appointed, and the COMMITTEE.

2.4. Personal data processing

Access to and processing of personal data in ITALFARMACO'S possession must be:

- in compliance with Italian Legislative Decree no. 196/2003, as amended, including regulatory amendments and additions, namely Regulation (EU) no. 2016/679 and Italian Legislative Decree no. 101/2018;
- only granted to authorised persons.

Confidentiality in the transmission of information is guaranteed.

2.5. Access to and use of the IT system

Access procedures require the use of passwords.

All employees and other authorised persons are informed that IT tools may only be used for company purposes.

Only IT system specialists are allowed to install software on personal computers.

3. Identification of sensitive areas, operations exposed to risk and the principles underlying the procedures

For the purposes of defining the system of internal controls, the areas sensitive to the commission of some of the offences set out in Articles 24 and 25 of the DECREE (offences against the public administration and against property committed to the detriment of the State or other public body or the European Union), some of the offences set out in Article. *24-bis* (computer crimes), some of the organised crime offences, including transnational ones, referred to in Article *24-ter* and Law no. 146 of 16 March 2006, the offence of introducing into the State and trading in products with false signs referred to in Article *25-bis*, some of the offences against industry and trade referred to in Article 25-*bis.1 of* the Decree, of some of the offences referred to in Article *25-ter of* the Decree (so-called corporate offences, including the offence of "bribery - and incitement to bribery among private individuals"), the offence of associations for the purposes of terrorism or subversion of the democratic order referred to in art. *25-quater,* the offences against the individual referred to in art. *25-quinquies ,* the offences of insider dealing and market manipulation referred to in Article 25-*sexies*, of the offences of manslaughter and serious or very serious negligent injury, committed in violation of the safety regulations and the protection of hygiene and health at work as per art. 25-*septies*, of the crimes of receiving, laundering, use of money, goods or other utilities of illicit origin and self-laundering referred to in art. 25-*octies,* offences relating to non-cash payment instruments and fraudulent transfer of valuables set out in Article 25-*octies.1,* some of the offences relating to breach of copyright referred to in Article 25-*novies,* offences against the administration of justice under art. *25-decies*, some of the environmental offences under art. *25-undecies,* the offences relating to racism and xenophobia under art. *25-terdecies*, tax offences under art. 25-*quinquiesdecies,* smuggling offences under Article *25-sexiesdecies* and offences against animals referred to in Article 25-*undevicies*.

.

The offences referred to in Article *25-quater*.1, the offences of fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited devices referred to in Art. *25-quaterdecies, offences* against cultural heritage referred to in Art. *25-septiesdecies*, offences of money laundering of cultural assets and devastation and looting of cultural and landscape assets referred to in Art. *25-duodicies* and some of the offences referred to in the categories of the previous paragraph have been analysed but, after a careful preliminary assessment, no specific opportunities for the commission of the offence have been identified with respect to them, since, although their abstract verifiability cannot be completely ruled out, their concrete realisation is unlikely, both in view of the Company's operational reality and in view of the elements necessary for the commission of the offences in question.

Within the areas of corporate operations, the following are identified by crime families:

- *sensitive* activities and operations for the commission of offences;
- the principles that must inform prevention and control procedures.

3.1. Crimes against the Public Administration (Articles 24 and 25 of the DECREE)

In accordance with Article 6 of the DECREE, within the scope of the *activities* that involve:

- relations with public officials, public servants, Supervisory or Control authorities, inspection organisations, public organisations that disburse aid, financing and soft loans, public service organisations and persons holding authorisation, granting, certifying or regulatory powers;
- participation in tenders or negotiations with public organisations for:
    a) the award or renewal of work under contract or concession;
    b) the performance of selection procedures, subcontracting authorisation, management of litigation with the client or control of compliance of services with the provisions of contracts, regulations or specifications;
- the management of public funds, in the phase of acquisition or disbursement of subsidies and in the performance of functions under concession;

the following *operations exposed to risk* are identified during whose performance or implementation the crimes under Articles 24 and 25 of the DECREE may be committed:

- participation in tender or direct negotiation procedures launched by public organisations or similar institutions;
- conclusion of contracts or agreements with persons classified as public and performance of the agreed services;
- application for and obtainment of qualifications, however they may be called, for the performance of a public service or essential public service;
- relations with persons classified as public in connection with the fulfilment of the requirements necessary to obtain and renew *concessions*, *authorisations*, *certifications* and *licences* for the ordinary performance of business activities;
- activities carried out by the COMPANY as an authorised provider of a public service or essential public service and relations with the recipients of these services;
- acquisition of aid, grants, financing, insurance and guarantees granted by public persons or organisations;
- management of relations with persons classified as public relating to property rights and the purchase and management of movable assets;
- relations with public persons, Supervisory and control authorities in fiscal and tax, corporate and financial, environmental, social security, welfare, health, occupational health and safety and accident prevention issues, as well as immigration or expatriation of people from other non-EU Countries;
- management of relations with the PA or with market and supervisory regulatory bodies, also in the case of inspections and audits;
- recruitment of personnel belonging to protected categories or subsidised or imposed recruits;
- relations with social security and welfare institutions;
- hiring of personnel who have recently had direct or indirect relations with the State, supervisory or control authorities, PA, including international, and European Union organisations;
- operations which, by their nature, are directly or indirectly related to the entities or organisations referred to in the previous point;

- operations that concern access to so-called social "shock absorbers" and employment contributions;

- hiring of external consultants;
- relations with the financial administration;
- relations with law enforcement authorities;
- marketing promotions and sponsorship of events in which persons classified as public take part;
- management of software belonging to persons classified as public or supplied by third parties on behalf of public persons;
- telecommunication or data transmission connections on IT or electronic media with the PA or other Authority.

With specific reference to the business operations of ITALFARMACO, the following transactions are identified as sensitive with respect to the commission of crimes against the Public Administration:

- supply contracts and free negotiations;
- direct selling to chemists;
- sales to dealers;
- gifts;
- management and distribution of drug samples and promotional media;
- donations and other charitable initiatives;
- scientific medical information activities;
- conclusion and performance of consulting agreements and partnerships with opinion leaders;
- management of congresses, conferences, seminars and investigator meetings;
- management of expenses claims and entertainment expenses;
- management of credit;
- tours of corporate laboratories;
- preclinical research activities;
- for-profit and not-for-profit clinical studies;
- activities connected with drug manufacturing;

- management of requests for authorisations, permits and licences;
- negotiation of the price of the drugs and definition of their pharmacotherapeutic group;

- drug traceability;
- relations with the PA concerning pharmacovigilance;
- application for public funding and management thereof;
- relations with the data protection authority (Garante);
- relations with the financial administration;
- customs and corporate compliance;
- purchase of goods and services;
- budget and management control;
- staff recruitment, training and incentives;
- management of agents, information systems, warehouses and depots, as well as trademarks and patents.

3.1.2 Principles underlying the procedures

Decisions of the senior executives and conflict of interest

The generation and implementation of their decisions are regulated by the law and by the provisions in the certificate of incorporation, Articles of Association, CODE OF ETHICS, MODEL and internal control system.

Directors are obliged to promptly inform the Board of Directors, the Board of Statutory Auditors and the COMMITTEE of all the positions they fill and the equity investments they hold - both directly and indirectly - in other enterprises, and of any terminations or changes that may lead to a conflict of interest under Article 2391 of the Italian Civil Code.

Executives are required to give the same information to the Managing Director and to the COMMITTEE.

The directors, General Managers and Executives of ITALFARMACO are obliged to disclose the existence of spousal or family ties, and the existence of present or former economic and financial ties with members of the PA or with suppliers, clients or third-party contractors of the COMPANY.

The same persons are required to abstain from accepting any gifts or gratuities not of a modest value from institutional contacts, contractual counterparties or in any case from persons with whom ITALFARMACO has business relations.

The COMMITTEE files and updates the information received.

Relations with the PA, with other authorities or with persons classified as public

Contacts with members of the PA must be specifically justified.

The COMMITTEE must be immediately informed of any unlawful or suspect proposals submitted by the PA or by persons classified as public.

Specific prevention and control procedures are in place and communications with public persons are traced in the scope of activities intended to obtain: administrative provisions, funding and public funds, authorisation to sell, negotiation of price and inclusion of drugs in formularies.

Specific procedures are in place to monitor:

- relations with the PA and the Authorities, with regard to pharmacovigilance, for the management of compliance and within the scope of auditing and control activities;
- relations with the AIFA for the inclusion of cases relating to congressional events;
- scientific medical information activities;
- management of credit and expenses claims;
- management of clinical studies, trials and product samples;
- participation in hospital tenders and in free negotiations.

In addition, it is forbidden to:

- Promising or making cash disbursements to representatives of the Public Administration, whether Italian or foreign, for purposes other than institutional and service purposes and in breach of company regulations;
- distribute gifts and presents to Italian and foreign public officials (including in those countries where the giving of gifts is common practice) or their relatives in excess of normal business or courtesy practices;

- promising or granting advantages of any kind (e.g. promises of employment, contributions, etc.) in favour of representatives of the Public Administration, whether Italian or foreign, in order to influence their independent judgement or induce them to secure any advantage for the company;

- incurring unjustified entertainment expenses for purposes other than the mere promotion of the corporate image, which are disproportionate to its purpose;

- favour, in purchasing processes, collaborators, suppliers, consultants or other third parties as indicated by representatives of the Public Administration, whether Italian or foreign, as a condition for the performance of subsequent activities;

- providing or promising to provide confidential information and/or documents;

- giving or promising money or other economic benefits to intermediaries as the price of their unlawful mediation, so that, by exploiting existing relations with public persons, they may intentionally exert an influence towards the PA aimed at influencing public action to the advantage of the Company;

- violate the duty of good faith in the performance of public supply obligations and contracts or, in the context of a public contract, fail to inform the PA of circumstances that have arisen during the performance of the work that entail a change in performance;

- Affecting or preventing the proper conduct of a tender procedure organised by the PA or diverting or preventing the free participation of other tenderers in the tender procedure by using violent means, threats, artifices, deception, lies or the giving of gifts or promises;

- altering the principle of free competition through collusive conduct between the individual participants in a competitive tendering procedure organised by the PA or an agreement with the person in charge of the tendering procedure;

Altering the procedure for the preparation of any act dictating the requirements and modalities for participation in a competitive comparison called by the PA, polluting its content and conditioning the manner in which the public administration chooses the contractor by using violent means, threats, artifices, deception, lies or collusive conduct or by acknowledging gifts or promises

Procedures are formalised to identify business functions outside the sales and marketing functions to express:

- an assessment of the scientific content of the operations, as part of the activities relating to the distribution of information and promotional material, professional development and scientific collaboration, the organisation of congresses, conferences and meetings, and tours of company laboratories;
- the pertinence to medical-pharmaceutical activity of modest value complimentary products;
- an opinion on the scientific content of the activities and projects to be financed in the context of the management of donations, research grants and scholarships payable by the COMPANY.

The recipients of the initiatives under the paragraph above must be alternated. Compliance with the principle is verified *ex post* on an annual basis.

Management of scientific consultations

Top management from different areas of the company must be involved in the activity: medical sales representatives and sales functions are not assigned a decision-making position.

A person in charge of the function requesting scientific advice is identified and has a coordinating role in the procedure. The Managing Director exercises control and authorisation powers.

Specific rules must be laid down for determining fair market value remuneration. It is possible to exceed the fee cap in exceptional cases, with written justification and an additional level of authorisation over and above the standard level.

The specific skills listed in the consultant's résumé must be relevant to the task to be performed and be commensurate with the intended level of remuneration.

The negotiation is assessed by a qualified company function independent of the proposing division.

There is an annual limit to the number of assignments and a fee cap for the consultant, except for exceptional and justified reasons.

The remuneration (or most of it) must be paid after the services have been provided in full, with positive results.

It is forbidden to make payments to persons other than the person who rendered the service or in countries other than the consultant's country of residence.
The consultancy contract is drawn up in writing and establishes: the object of the consultancy; the terms and conditions of the service and payment; the consultant's disclosure obligations towards the company and third parties.

3.2. Cybercrimes (Article 24-*bis* of the DECREE)

In accordance with Article 6 of the DECREE, within the scope of activities that involve the direct or indirect use of IT or telecommunications systems, the following operations exposed to risk - during whose performance or executions the crimes under Article 24-*bis* of the DECREE may be committed - are identified:

- management of the user profile and the authentication process, external logins, as well as system outputs and storage devices;
- management and protection of the workstation;
- classification and processing of operations;
- identification of roles and procedures;
- protection of software, content, network and transmissions;
- monitoring of computer processing activities;
- control of logins;
- operational continuity security;
- legal (copyright) and technical compliance policy;

- management and protection of the networks;
- development of the general IT security guidance plan and specific management activities;
- relations with external parties by means of IT systems;
- online transactions;
- physical safety, in particular of cabling, network devices, premises and equipment;
- classification and use of the assets;
- reporting of critical security events;
- procurement and development;
- maintenance of HW-SW products.

3.2.1. Principles underlying the procedures Management of the IT tools

a) *Confidentiality and access to data*

Confidential information must be protected when saving, storing and forwarding, so that it is accessible only to persons authorised to process it (the so-called confidentiality principle).

The following is envisaged:

- a protection system capable of uniquely identifying the users accessing a processing or transmission system;
- a system to control the use of resources by processes and users, through the management and verification of access rights. These are authenticated before any additional operational interaction with the system. Only authorised users can save and access the corresponding information.

b) Integrity of data

It is ensured that the company data corresponds to those originally entered into the IT system or altered legitimately. The information must not be tampered with by unauthorised persons (integrity principle).

c) Availability of data

Company data must always be available in accordance with the requirements of process continuity and in compliance with the rules that require historical storage (availability principle).

d) Non-repudiation

Specific measures are applied to assure that processes can always be controlled, also in terms of traceability to specific persons (non-repudiation).

e) IT security: vulnerability checks

Resources and corresponding vulnerabilities, or deficiencies in protection against a certain threat are identified and classified in relation to the following component parts: infrastructures (including technological, such as networks and systems); hardware; software; documentation; data and information; human resources.

Internal and external threats are grouped by type as follows: errors and malfunction; fraudand theft; harmful software; physical damage; system overload; failure to comply with applicable legislation.

IT security activity must be planned and periodically updated, establishing a system of preventive protection.

The following is prepared:

- a corporate policy that establishes how users can access applications, data and programmes;
- a set of control procedures designed to verify access authorisations and that the rules for disabling inactive ports are working properly.

Potential damage that could be caused by the threats are identified, considering the likelihood of them occurring and possible countermeasures.

A preventive and corrective action plan is defined and updated periodically on the basis of the risks to counteract. The residual risk is documented and expressly accepted.

f) IT security: monitoring the correct use of tools

Periodic spot checks are made to monitor the correct use of the IT and telecommunications tools by internal and external persons. These checks must be recorded.

g) IT security: continuity in IT services

An emergency system is in place, defining technical and organisational procedures to address this. Operational continuity is guaranteed through mechanisms designed to overcome anomalous situations.

If data transfer protection media are unavailable, processes are in place to ensure that the resources are quickly restored in order to guarantee confidentiality, integrity and availability to transmission channels and networking components.

h) IT security: recording IT events

A system to track and monitor IT events and network security actions is in place.

i) IT security: analysing IT events

The recorded events are analysed to detect anomalies that, deviating from the established standards, thresholds and procedures, could be indicative of threats.

j) Data: security backup

Data is backed up at fixed intervals.

k) *Data: quality control*

Oversight procedures are in place for the preventive control and ongoing monitoring of data quality and HW-SW performance.

l) Physical security: server rooms

The physical security of the sites where the IT systems reside is ensured and a system for managing physical credentials (badges, pins, access codes, token authenticators, biometric values) is in place.

m) Procedures, operating instructions and management of accounts The creation, modification and cancellation of accounts and profiles is regulated.

Only authorised personnel must know the passwords or login codes for computers, which must be changed regularly.

Procedures are formalised for allocating special privileges, such as system administrators or super users.

n) Logical and physical inventory of hardware and software

An inventory is taken of the hardware and software available to users; it is periodically updated.

A corporate management and control policy of the physical security of the environments and resources is prepared and includes precise knowledge of the tangible and intangible assets being protected (technological resources and information).

o) IT security: Access Log

The system administrators in the manufacturing premises regularly review the access logs. System operators are only allowed to access the systems and/or data that they are required to work on. user access to the company network and applications is tracked and controlled.

p) IT security: access to manufacturing premises

Separation of development, test and manufacturing premises is guaranteed.

The personnel involved in the development of applications are not allowed to access the manufacturing premises.

q) IT security: encryption

Encryption controls are used to protect information and the process of generating, distributing and storing keys is regulated.

r) IT security: digital signature

The use of digital signatures is regulated for documents referring to the responsible person, authorisation levels, certifications systems, as well as the use and forwarding of files with storage procedure.

s) Data: reuse of storage media

Tools are in place for the safe reuse of storage media.

t) *Privacy activities and regulations*

Minimum safety measures are adopted for personal data processing using electronic equipment, including authentication and authorisation systems, antivirus and backup.

A personal data processing risk assessment is carried out every year, together with an audit to identify exposed areas plan security measures.

u) Operating instructions and procedures: security policy for in-house staff

Information protection policies are in place with reference to:

- log-in and log-out procedures;
- the use of passwords, electronic mail, removable media and protection systems (antivirus, antispam, antiphishing, antispy).

v) Procedures and operating instructions: Behavioural prohibitions for internal staff

Internal staff are expressly prohibited from:

- Producing, using, altering or counterfeiting false electronic documents (such as deeds, certificates, authorisations), including for the purpose of certifying data that is untrue
- destroy, suppress or conceal computer documents, in any form and for any purpose;
- forcing third parties, through the use or threat of IT tools or illegal digital behaviour, to perform or omit acts in violation of current legislation or contractual obligations.

w) Suppliers of IT services and products: managing relations

IT security training is organised for the users and for certain professionals.

Technical documents are prepared explaining proper use of the IT system and for effective security management by the corporate functions.

x) IT service and product providers: relationship management

Relations with suppliers of IT services are regularly controlled. Appropriate protective provisions are included in the contracts.

y) Suppliers of IT services and products: controls and outsourced services

IT assessments are periodically prepared, in particular for outsourced services.

z) Audits

The roles, responsibilities and operating procedures for the periodic audits of the efficiency and effectiveness of the IT security management system are regulated.

3.3. Counterfeiting money crimes (Article 25-*bis* of the DECREE); crimes against industry and trade (Article 25-*bis*.1 of the DECREE) and copyright infringement and related offences (Article 25-*novies* of the DECREE)

A. In accordance with Article 6 of the DECREE, within the scope of activities in the performance of which conduct that could endanger the certainty and reliability of money movements could occur, the following operations exposed to risk are identified at the COMPANY:

- introduction into the Italian State, possession, handling and use of Italian or foreign currency and revenue stamps;
- availability of funds in cash or valuables;
- research and development of new technologies.

B. Within the scope of management activities of:

- the manufacturing and distribution process;
- relations with customs officers for the export and import of industrial products;
- relations with regulatory bodies, anti-adulteration units of the Italian military police (NAS Carabinieri) and State Police authorities during inspections of the manufacturing process, the release of batches on the market or to issues concerning product traceability;
- substances or products submitted to specific regulations and corresponding compliance, controls and inspections by the oversight authority;
- relations with public persons to obtain authorisations, licences and concession to perform the corporate business and run the manufacturing plants;

- approval, certification and declaration of conformity by bodies and institutes, also during audits;
- relations, compliance and communications with AIFA and other regulatory bodies regarding authorisation and verification processes for the import and manufacture of pharmacologically active substances, compliance with Good Manufacturing Practices and product marketing authorisations;
- the requirements laid down by the Pharmacovigilance system;
- national or international business that may involve interactions with authorities or the PA;
- patents and trademarks;
- IT or telecommunications resources and information or any other intellectual property protected by copyright;
- agents and business partners;

the following *operations exposed to risk* are identified at the COMPANY, during whose performance or implementation the crimes under Articles 25-*bis*.1 and 25-*novies* of the DECREE may be committed:

- production, use and circulation of products that violate industrial property rights or ownership;

a) preparation and communication of documents and information intended for public and regular officials and bodies for:obtaining authorisations for the production, marketing and import of pharmacologically active products;

b) controls, particularly of compliance with Good Manufacturing Practices;

c) other regulatory activities relating to the preparation of documentation, the progress and conclusion of the authorisation process and the control activities;

d) compliance with pharmacovigilance requirements or during audits or inspections at the COMPANY;

e) the development of international projects;

f) the filing of patents and trademarks and the management of the granting and registration procedures;

- the management of pharmaceutical labels;
- activities connected with the purchase and use of software and databases;
- the use and dissemination of information materials relating to scientific research or other copyright protected content.

3.3.1. Principles underlying the procedures

Compliance with the protection of industrial property rights and copyright and prevention of crimes of forgery

Prior to marketing of the products (including those imported or licensed by third parties) or their manufacture in States which recognise industrial property rights, the existence of any patented inventions, trademarks and non-patented but secret, substantial and identified know-how is verified.

The controls are managed by the Legal Department of the COMPANY.
The controls, accompanied by a written opinion of the Legal Department and any external consultants, are sent to the Managing Director for the final decision. Periodic audits of the research and development of new technologies are performed.

The filing of applications to patent an invention or register a trademark must be preceded by controls of the existence of rights in the country of interest, to ensure compliance with the requirements of innovation and inventiveness, as regards patents, and of originality and no risk of confusion for trademarks.

Any administrative or legal appeal or challenge against other patents or trademarks shall be preceded by controls confirming the illegality or invalidity of such rights and must be approved by the Managing Director with the favourable opinion of the Legal Department.

Patent applications are processed by the Research Department of the COMPANY; trademarks are processed by the relevant commercial or licensing sectors.

Applications and candidate trademarks, accompanied by the opinion of the Legal Department regarding the controls carried out, are sent to the Managing Director for a final decision.

If it is not possible to carry out adequate checks before the decision is taken for reasons of urgency, the filing of the application shall be subject to an adequate justification of the exemption shared with the Legal Department.

Non-patented, confidential know-how, received from third parties on the basis of secrecy or other agreements, may be communicated within the COMPANY, only on a need-to-know basis to the qualified persons involved in the evaluation or use of the information (need-to-know principle).

The dissemination of publications, including abstracts or copies thereof, may be ordered by the company department concerned after verification by the Legal Department of compliance with copyright regulations.

Special procedures are in place for the acquisition and management of software licences and pharmaceutical labels.

Guarantee of nature, quality, conformity of marketed products

Control and monitoring mechanisms are in place for the manufacturing process, in particular to ensure that the product delivered to the purchaser corresponds in nature, origin, quality and quantity to that declared or agreed upon.

3.4. Corporate crimes (Article 25-*ter* of the DECREE) and Market abuse (Article 25-*sexies* of the DECREE)

In accordance with Article 6 of the DECREE, the following operations exposed to risk in the COMPANY, during the performance or execution of which, the crimes under Articles 25-*ter* and 25-*sexies* of the DECREE may be committed, are identified:

- recognition, recording and representation of the COMPANY'S business activity and of the economic, financial and equity position in the accounting entries, financial statements, reports and other documents intended for the COMPANY, the Supervisory or Control Authorities, the market or third parties, especially on the occasion of extraordinary operations;
- organisation and participation in meetings and management of relations with the Supervisory or Control Authorities, representatives of the State Administration, journalists and other representatives of the mass media;

- preparation of the financial statements, the consolidated financial statements, reports and other communications required by law and intended for the shareholders or the public, and the associated evaluation of the provisions for risk;
- relations with the Board of Statutory Auditors, independent auditors and shareholders;
- relations with consultants in extraordinary transactions and financial intermediaries;
- documentation, filing and storage of information relating to the operations and transactions referred to in the previous points;
- conflict of interest of directors, general managers, managers in charge of drawing up accounting documents or in charge of purchase or sale reports;
- management of financial resources, accounting and cost centres;
- preparation and running of shareholders' meetings;
- allocation of profits;
- securitisation of receivables;
- transactions on share capital, ITALFARMACO shares or equity interest in controlled undertakings or undertakings outside the GROUP;

- purchase, sale or other transactions involving unlisted financial instruments or for which a request for admission to trading on a regulated market has not been submitted;
- conclusion of derivative instruments not traded on Italian and European regulated markets.

3.4.1. Principles underlying the procedures

Recognition, recording and representation of the business activity in the accounting entries, financial statements, reports and other documents

Appropriate measures are taken in each functional structure or organisational unit to ensure that:

- accounting operations are carried out in compliance with the principles of truthfulness, completeness and accuracy;
- any anomalous situations are promptly reported;
- the information provided to higher ranking persons is truthful, correct, accurate, timely and documented, also using computerised methods.

The function manager who provides information about the financial statements or other corporate disclosures takes responsibility for the completeness and truth of the data transmitted.

The COMMITTEE must be immediately informed if unjustified requests are made to change already booked data and the criteria used for recognising, recording and representing the accounts.

A person responsible for controlling the information provided by the company for the purpose of preparing the consolidated Financial Statements is identified. The companies in the GROUP that provide this information are required to certify the truth and completeness thereof.

Anyone who provides information to higher ranking units is required - to specify the sources and make copies of the documents available, where possible, if this aids in comprehension

of the information, and is requested.

Corporate activities

Appropriate procedures are formalised to oversee extraordinary operations and the management of the obligations relating to the functioning of corporate bodies and relations with control bodies.

Extraordinary operations are reserved for the BOD, which may adopt specific measures or grant powers of attorney to define the procedures for their execution.

Purchase, sale or other transactions involving: unlisted financial instruments or for which a request for admission to trading on a regulated market has not been submitted; conclusion of derivative instruments not traded on regulated markets

A policy on financial investment management and related risks is formalised.

Unlisted financial instruments that may be the subject of transactions by ITALFARMACO, including through subsidiaries, are identified.

The persons empowered to decide on transactions relating to the conclusion of derivative contracts, implementing them and carrying out control and supervision activities are specified. The BOD must authorise the transactions, without prejudice to the contents of the powers of attorney conferred.

Counterparties with which transactions may be carried out and the limits for the management of investments and related risks must be identified.
If the trading counterparty is not a financial intermediary subject to prudential oversight, fairness and transparency in compliance with European Union legislation, the function responsible for the decision must justify the transaction and the price established.
Derivative contracts are entered into according to models recognised by international best practice (ISDA).

Transactions in listed financial instruments

The following are identified:

- the instruments that may be the subject of transactions by the COMPANY;

- the persons empowered to authorise, decide and implement the transactions, as well as to control and supervise them;
- the counterparties with which transactions may be carried out and the limits established for the management of investments and related risks.

3.5. Crimes committed for the purpose of terrorism or subversion of the democratic order (Article 25-*quater* of the DECREE), crimes against the individual personality of people, aiding and abetting illegal immigration and employment of illegally resident non-EU nationals (Articles 25–*quinquies* and 25-*duodecies* of the DECREE), and crimes of racism and xenophobia (Article 25-*terdecies* of the DECREE)

A. In accordance with Article 6 of the DECREE, within the scope of activities that involve the risk of establishing relationships with counterparties, customers or persons and there is reason to suspect that they pursue or facilitate, directly or indirectly, terrorism or subversion of the constitutional order, the following operations exposed to the risk of committing the crimes referred to in Article 25-*quater* are identified in the COMPANY:

- contractual relations with counterparties resident or operating in countries considered at risk;
- management of humanitarian and solidarity initiatives, in particular for the benefit of entities based or operating in countries considered at risk.

B. Within the scope of the management of human resources and activities that involve the risk of establishing relations with suppliers or customers where there is reason to suspect that they pursue or facilitate initiatives aimed at the exploitation of persons or child pornography, or the transport or illegal entry of foreigners into the Italian State, or into another State where the person is not a citizen and/or does not have the right to permanent residence, the following operations exposed to the risk of committing the crimes referred to in Article 25-*quinquies* and Article 25-*duodecies* of the DECREE are identified in the COMPANY:

- contractual relations with counterparties resident or operating in countries considered at risk or that in Italy use citizens from other countries who require a permit to stay;
- management of IT or telecommunications media;

- realisation and management of humanitarian and solidarity initiatives, in particular for the benefit of entities based or operating in countries considered at risk.
- recruitment and management of non-EU personnel and human resources.

C. In accordance with Article 6 of the DECREE, the following operations exposed to risk are identified in the COMPANY, during whose performance or implementation the crimes under Article 25-*terdecies* of the DECREE may be committed:

- human resources management;
- use and dissemination of information, including by means of IT equipment;
- donations, sponsorships and management of initiatives in support of entities.

3.5.1. Principles underlying the procedures

Selection of suppliers, business counterparties, and partners

Suppliers of goods or services are selected by the relevant function on the basis of requirements of professionalism, reliability, cost-effectiveness, equal treatment and transparent selection procedures.

The minimum requirements and evaluation criteria are defined before the receipt of proposals.

A supplier qualification and certification procedure is in place and takes into account: the conformity of the object of the supply with the procurement specifications; the best available technologies in terms of environmental protection and workplace health and safety.

The principle of cost-effectiveness can never prevail over the criterion of reliability.

The criteria for the selection, conclusion and performance of agreements or joint ventures with other companies for the realisation of investments are predetermined.

Careful assessment is made of possible business partnerships with companies that:

- operate in the sectors of telecommunications (in relation to the risk of spreading child pornography) or tourism in at-risk geographical areas;

- operate or are based in areas considered at risk due conduct for the purpose of terrorism.

Regulation of relations with suppliers, consultants, contractual counterparties and partners

A specific provision is included in the contracts with business counterparties, consultants and partners where they declare:

- that they are acquainted with the DECREE and undertake to comply with it;
- in the case of companies, that they have adopted the organisational Model in accordance with the DECREE or an equivalent document or an adequate system of control procedures.

A specific provision is included in the contracts with commercial counterparties, consultants and partners that regulates the consequences of violation of the DECREE (e.g. express termination clauses or penalties).

Whenever the contracts governing relations with the company so permit, compliance by suppliers and partners with applicable labour legislation is checked, paying special attention to child labour and hygiene, health and safety.

Selection of employees, agents, consultants and collaborators

Employees, consultants and collaborators are selected by the function managers of the COMPANY.

The decision must be justified on the basis of the professional requirements of the position or job to perform and in compliance with the principles of equal treatment and independence.

The profile of the resource to be selected must be defined before commencing the interviews.

The process of selecting applicants must include at least two interviews:

- the first one conducted by external consultants or by Human Resources;
- the second, of a specialist nature, with the head of the department interested in recruitment or with the Managing Director.

The selection "interview" form is filled in, summarising the characteristics of the applicant. Hiring is governed by a regular employment contract, in compliance with all applicable regulations and collective bargaining agreements.

The relevant departments must verify that the person with whom the employment relationship is to be started or consultancy, agency or tender contracts are concluded meets the legal requirements for staying and working in Italy.

A procedure for hiring is formalised: a privacy statement must be provided and a declaration of consent to the processing of personal data must be signed; a certificate of criminal records is required.

Staff training

Employees (and COLLABORATORS, if the contractual arrangements allow it and the COMPANY can exercise executive and control power) shall be trained and constantly updated about the rules and controls in place for the prevention of OFFENCES.

Remuneration and bonus system

Any bonus systems for employees and collaborators must correspond to realistic goals that are consistent with the tasks and activities carried out, as well as with the responsibilities entrusted to them and the operational structure available.

Fees or commissions may be envisaged and paid to consultants, collaborators and persons classified as public, provided that they are commensurate with the services rendered and the task assigned. This must be assessed on the basis of reasonable criteria and in accordance with the conditions and practices existing in the geographical area of reference or determined by rates.

The organisation of trips or periods spent in foreign locations is regulated with specific regard to the principles of morality and the risk of committing the offences referred to in Articles 25-*quater* and 25-*quinquies*.

3.6. Crimes against the delivery of justice (Article 25-*decies* of the DECREE)

In accordance with Article 6 of the DECREE the following operations exposed to risk are identified, during whose performance or implementation the crimes against the delivery of justice may be committed:

- management of in-court and out-of-court disputes;
- relations with persons involved in court proceedings or preventive measures.

3.6.1. Principles underlying the procedures

Management of assignments for legal services

Preventive controls are in place for the provision of legal assistance and advice and monitoring and verification of the services provided.

3.7. Organised crime, including transnational, and money laundering (Articles 24–*ter* and 25–*octies* of the Decree and Italian Law no. 146 of 16 March 2006)

With reference to the risk of establishing relations with physical or legal persons for whom there is reason to suspect that they are directly or indirectly engaged in illegal activities as set forth in Article 25–*octies* of the DECREE and Italian Law no. 146/06, the following sensitive operations are identified in the COMPANY:

- intercompany investments, loans and financial transactions and cash flow management activities;
- acquisition and disposal of companies or company units, as well as the establishment of temporary groupings of companies and *joint ventures*

- activities of:
    a) appraisal, qualification and selection of suppliers of goods and services;
    b) evaluation of clients and definition of credit limits;
    c) management of the economic and financial conditions included in contracts with customers and suppliers (such as advances to suppliers, payment and collection terms and conditions);
    d) reminders and credit recovery;
- realisation and management of humanitarian and solidarity initiatives, in particular for the benefit of entities based or operating in countries considered at risk;
- donations to associations, local and state entities and sponsorships of events and sports clubs;
- management of IT and telecommunications media;
- activities involving risks of:
    a) engaging in conduct liable to constitute, even as a competitor, offences of criminal conspiracy, including mafia-type offences, or for the purpose of tobacco contraband or illicit trafficking in mood-altering or psychotropic drugs;
    b) allow or facilitate customers or counterparties, directly or indirectly, to launder money, goods or other benefits or to use them, if they are of illegal origin;
    c) have contacts, even indirectly, with organised crime syndicates.

Within the scope of those activities, the following operations exposed to risk are identified in the COMPANY:

- recourse to techniques for the splitting of transactions or payments;
- transactions involving large amounts, uncommon with respect to those normally undertaken by the customer;
- frequent transactions by a customer in the name or on behalf of third parties, when the relations do not appear to be justified;

- transactions made by third parties in the name or on behalf of a customer without plausible justification;
- request for transactions with clearly inaccurate or incomplete information;
- management of import and export and marketing of mood-altering or psychotropic drugs;
- transactions with counterparties operating in geographical areas known as off-shore centres or areas of drug trafficking or tobacco contraband, which are not justified by the customer's business activity or other legitimate circumstances;
- requests to exchange banknotes with others of different denominations or currencies;
- transactions involving the use of electronic money whose amount or frequency is not commensurate with the customer's business activity or normal use of the instrument;
- use of letters of credit and other commercial financing systems to transfer money from one country to another, without the transaction being justified by the customer's customary business activity;
- trustee title to financial assets or instruments that have been in the possession of the business partner for a short time, which is not justified by the customer's equity position or business activity.

3.7.1. Principles underlying the procedures

Management of financial resources

Caps are set on the autonomous use of financial resources, by setting limits consistent with the management powers and organisational responsibilities assigned.

The supplier payment process must be formalised and based on the principle of segregation of duties, for which different persons must perform supplier registration, invoicing and payment.

Procurement management must be centralised. Transactions involving the use of economic resources (such as the acquisition, management and transfer of cash and securities) orfinancial resources must have an express purpose and be documented and recorded in accordance with the principles of professionalism and sound management and accounting.

It must be possible to verify the decision-making process. The applicant must justify the use of financial resources and confirm their appropriateness.

The formal and material provenance of cash and securities is identified.

Acquisition, management and transfer of cash or securities must be documented at every stage, by the relevant departments, so that all the persons involved can be identified.

Whoever handles cash or securities on behalf of the COMPANY is required to comply with the internal procedures for detecting and reporting forgeries and for controlling securities.

Anyone who ascertains or suspects a forgery or alteration of cash or securities must immediately suspend the transaction and inform the person in charge of the procedure and the COMMITTEE thereof.

The identity of the recipients or originators of the payments with the counterparties of the transaction is verified.

For every purchase, Accounts must:

- ensure that the contract or purchase order, invoice and transport documents correspond;
- verify the actual delivery of the goods or supply of the service with the Function that issued the order;
- record the transaction.

The employee must be authorised by the manager for reimbursement of expenses incurred while performing their job. The reimbursement is credited by bank transfer at the same time as wages are paid.

The types of EMPLOYEE expenses that may be reimbursed must be expressly regulated.

Formal and substantial controls of payments to third parties and for intra-group transactions are carried out. The checks take into account: the registered office of the counterparty company and the banks involved in the transactions, as well as institutions that do not have physical establishments in any Country; any corporate screens and trust structures used for extraordinary transactions and operations.

Relations with financial intermediaries

In order to implement decisions concerning the use of financial resources and transactions involving the acquisition, management or transfer of cash or securities, the COMPANY uses financial and banking intermediaries subject to transparency and fairness regulations in compliance with European Union regulations.

Financial operators must possess manual and computerised safeguards to prevent money laundering.

It is forbidden to: use cash for collection, payment, transfer of funds, employment or other use of financial assets; execute payment orders received from persons who cannot be identified.

Payments for goods and services purchased by the COMPANY must correspond to the provisions of the contract and are made exclusively to the current account in the supplier's name.

Unless adequate justification of the legitimacy and congruence of the operation is provided, payments are prohibited:

- to numbered current accounts or to banks belonging to or operating in countries listed as "tax havens", or to offshore companies;
- to a party other than the contractual counterparty or who is in a different Country from that of the contracting parties or the country of performance of the contract.

Knowledge of clients and identification of suspicious transactions

There is an obligation to investigate and update knowledge of the counterparty in order to assess the consistency and compatibility of the transaction with their economic and financial profile.
The commercial and professional reliability of customers is checked on the basis of a number of relevant indicators such as: the acquisition of commercial information on the company, shareholders and directors through specialised companies, the involvement of politically exposed persons pursuant to Article 1 of the Technical Annex of Italian Legislative Decree no. 231/07.

Any anomalous or suspicious transactions by counterparty, type, object, frequency or entity are immediately reported to the COMMITTEE.

In the event of anomalous profiles in financial relations with the supplier or customer, the relationship may only be maintained with the express authorisation of the Managing Director.

Immediate reporting is required of:

- transactions carried out by a person in the name of, on behalf of or for the benefit of third parties, in the absence of family ties or business relationships that justify them;
- transactions carried out by third parties for the benefit of counterparties, in the absence of justifying reasons.

The elements to be considered in the evaluation of a suspicious transaction are:

- the amount of the transaction;
- the method of execution;
- the recipient of the transaction;
- the territorial location.

Personnel in direct contact with customers must report any elements that make the transaction suspicious to the Function Manager.

Special procedures are formalised to monitor import and export activities and the marketing of mood-altering or psychotropic drugs and substances.

Management of cash transactions ordered by customers

The processing of cheques is formalised with multiple checks.

Management of the process of procurement of goods and services

There must be no subjective identity between the person requesting the performance, authorising it and making the payment. The tasks, powers and responsibilities attributed to each person are formalised.

The following must be envisaged:

- a function or unit responsible for defining the technical specifications and evaluating offers;
- the appointment of a person responsible for contract performance (the so-called contract manager) specifying the tasks, powers and responsibilities attributed to them;
- authorisation for substantial modifications, additions or renewals of the contract by a superior of the contract manager;
- the prohibition, in respect of suppliers or consultants, to assign to third parties the right to perform the service stated in the contract and to collect the remuneration, as well as to assign the right to collect it to third parties.

Transfers of corporate assets

For the acquisition and disposal of companies or company units, the origin of the assets contributed to the assets of the company or company units to be acquired is verified in advance, in addition to the identity, registered office, legal nature and anti-mafia certification of the assignor.

3.8. Workplace health and safety offences (Article 25-*septies* of the DECREE)

Within the scope of the sectors of activity and production units where workers are employed (including employees of external or self-employed companies to which the COMPANY entrusts contract or subcontract work), the following sensitive activities are identified with reference to the offences provided for in Article 25-*septies* of the DECREE:

- planning and management of health and safety prevention and protection for workers;
- identification, assessment and mitigation of risks, in particular the periodic assessment in order to:

a) identify health and safety hazards in the performance of the assigned tasks;

b) identify the measures in place for risk prevention and control;

c) define the plan to implement new measures as the need arises;

- organisation of company structures in terms of workplace health and safety: in particular, definition of tasks, functions and responsibilities; analysis, planning and control activities; participation of internal and trade union bodies; preparation of work rules and procedures; scheduling of maintenance activities, tests and personal protective equipment; management of emergencies, first aid and health surveillance;
- system of delegations of functions;
- information activities aimed at achieving, at all company levels, constant attention to safety and health;
- training activities, in particular the implementation of systematic training and awareness-raising plans for employees, as well as refresher courses for people with a specific role in relation to safety and hygiene requirements;
- relations with suppliers involved in the management of workplace health and safety or with other suppliers, planners, manufacturers, installers or persons with whom contracts, works or supply contracts exist;
- maintenance and care of movable and immovable property;
- systematic and continuous monitoring of data and indicators of the various corrective operations and actions;
- management of control mechanisms (such as audits and inspections) to verify the:

a) correct application of policies, programmes and procedures;

b) clear definition, understanding, sharing and operation of organisational responsibilities;

c) conformity of raw materials, equipment, plants and industrial activities with laws, regulations and internal rules;

d) identification of any discrepancies and the implementation of corrective actions;

e) identification and control of known risk situations;

f) assurance of long-term continuity of the compliance of plants, assets and equipment;

g) control, recording and monitoring of the impact of the industrial activity on the health of personnel.

3.8.1. Principles underlying the procedures

Planning of the prevention and protection service

The prevention and protection service is established in accordance with Italian Legislative Decree no. 81 of 9 April 2008.

A budget, annual and long-term investment plans and specific programmes are drawn up in order to identify and allocate the resources needed to achieve health and safety targets.

The following are envisaged: a prevention and protection plan, implementation methods and a periodic monitoring system.

The roles, responsibilities and management methods of the prevention and protection service are regulated.

In accordance with the provisions of the law, the COMPANY establishes:

- the assessment and periodic monitoring of the suitability and professionalism requirements of the person in charge and of the prevention and protection service employees (Health & Safety Officer [RSPP] and Health & Safety Department [SPP]);
- the minimum skills, number, tasks and responsibilities of the workers involved in the implementation of emergency, fire prevention and first aid measures;
- the process of appointment and acceptance of the Occupational Health Physician, as well as the duration of the appointment and procedures governing succession in the role.

Identification, assessment and mitigation of risks

A procedure for the preparation of the Risk Assessment Document (Documento di Valutazione dei Rischi -DVR) is defined and envisages:

- identification of the competent persons;
- the drafting procedures;
- responsibilities for verification and approval of the contents;
- monitoring of the implementation and effectiveness of the actions taken, in order to examine the risks and update the document.

Management of the prevention and protection service

Procedures are defined for the preparation and implementation of the prevention and protection system. In particular, the following is envisaged:

- the recording of the results of workers' health checks in the Health and Risk Records;
- the management, distribution and maintenance of personal protective equipment (PPE);
- the procedures for appointing workers responsible for implementing prevention, emergency and first aid measures;
- the rules for the management of safety signage;
- requirements for workers' access to risk areas;
- operating procedures, roles and responsibilities in the event of an emergency;
- procedures for leaving the workplace or a hazardous area in the event of serious and immediate danger;
- the timing and procedures for applying for the issue or renewal of the fire prevention certificate and provisional authorisation.

Checklists are prepared for the adoption of accident prevention measures, including: critical operations, products and equipment; processes with an impact on the health and safety of workers; PPE shared with the person in charge of the prevention and protection service.

An emergency management plan and procedure to mitigate the effects on health and the external environment is defined and tested.

Specific procedures have been established for the management of accidents, which include: identification of the types of accidents at work on the basis of current legislation; definition

of roles, responsibilities and operating procedures for the preparation and completion of the accident log; analysis of the causes of accidents for the adoption of the necessary preventive measures.

Roles and responsibilities are established, with the participation of the Occupational Health Physician and the RSPP, for defining and implementing appropriate organisational methods to protect workers. The risks associated with the activities carried out, the work environment, the use of equipment and machinery, the use of hazardous substances and chemical, physical, biological and carcinogenic agents are considered.

The fire risk must be assessed and an emergency plan and a fire prevention register are prepared and updated.

Monitoring

A procedure for systematic and continuous monitoring of the activities constituting the health and safety prevention and protection system is prepared and establishes:

- roles and responsibilities;
- the definition of specific performance indicators for the management of the Prevention and Protection System that permit an evaluation of effectiveness and efficiency;
- the analysis and implementation of corrective actions in the event of any system weaknesses.

The procedure must provide for the detection, recording and investigation of actual accidents and near-misses and of potentially harmful situations.

Audit activities in the field of health and safety of workers

The following are regulated:

- the scope, frequency, methodology, requirements, competencies, roles and responsibilities for the conduct of audit activities;

- the recording and communication of the results of the application of technical and organisational solutions for safety management, according to legal and company requirements;
- systematic verification of the state of implementation and effectiveness of the measures adopted to neutralise the risks;
- corrective actions in the event of shortcomings or deviations from the requirements;
- roles, responsibilities and operating procedures for periodic reporting to the Managing Director and the COMMITTEE on the system evaluation activities.

Engagement of personnel in the field of health and safety of workers

The following is envisaged:

- regular meetings with management, workers and their representatives;
- prior consultation with workers' representatives regarding the identification and assessment of risks and the definition of preventive measures.

Training of personnel in the field of health and safety of workers

Employees are provided with an internal policy document setting out the guidelines and objectives of the prevention and protection system aimed at pursuing adequate health and safety protection.

A procedure is formalised to regulate roles, responsibilities and operating procedures for training and updating workers, as well as for communicating information, also in the event of serious and immediate danger.

Periodic meetings of the officers in charge of health and safety management control are scheduled.

The Occupational Health Physician must be given information about the processes and risks associated with manufacturing activities.

Maintenance and inspection of movable and immovable property

A procedure is drawn up to regulate the activities and reports on maintenance and inspection of company assets to ensure compliance with workplace safety and hygiene regulations.

3.9. Offences relating to non-cash payment instruments and fraudulent transfer of values (Article *25-octies*.1 of the DECREE)

The following sensitive activities have been identified at the COMPANY, in the performance or execution of which the offences referred to in Article 25-octies.1 of the DECREE may be committed:

- management of financial flows;
- management of in-court and out-of-court litigation

3.9.1. Principles informing procedures

- The following general principles of conduct apply to the addressees of this Model who, in any capacity, directly or indirectly, are involved in the above-mentioned operation at risk with respect to offences relating to non-cash payment instruments and fraudulent transfer of valuables.
- In general, such persons are prohibited from:
- using credit cards or any other payment instrument enabling the withdrawal of cash or the purchase of goods and/or the provision of services, for oneself or for others, for the purpose of profiting therefrom, unduly and without being the holder thereof;
- fraudulently, knowingly and without right using an instrument of payment, including an instrument other than cash, which has been stolen or otherwise unlawfully obtained or unlawfully appropriated;
- forging or altering instruments of payment, including those other than cash, or possessing, disposing of or acquiring such instruments or documents of unlawful origin, or in any event forged or altered, as well as payment orders produced with them;

- transferring the ownership and availability of money, assets, profits, company shares or other values to fictitiously interposed third parties in order to evade the application of the confiscation , seizure or other measures of patrimonial or smuggling prevention, even where the prevention measure has not yet been orderedevade the provisions on anti-mafia documentation by fictitiously attributing to others the ownership of companies, company shares or shares or corporate offices, when participating in procedures for the award or execution of contracts or concessions; transferring the ownership or availability to fictitious holders of money, goods or other assets and proceeds of unlawful origin in order to facilitate their reinvestment in productive activities.
- In addition, as a general rule, all criminal conduct against public faith, property, or which in any case offends property, is prohibited when it relates to non-cash payment instruments. Furthermore, such persons are required to:
- Ensuring, in the use of payment instruments, including non-cash, the freedom of the digital single market, avoiding any form of obstacle or threat to consumer confidence and forms of direct economic loss;
- use on behalf of the Company only payment instruments owned by the Company;
- define the payment methods provided for the purchase of goods or provision of services as well as adopt appropriate control instruments to ensure that such payment instruments are not counterfeited and/or altered;
- ensure that 'digital' payments are processed through the adoption of security procedures and over reliable communication infrastructures;
- make cash withdrawals in compliance with the sector regulations on the use of cash and with the document/authorisation system in force in the company;
- use payment instruments with adequate security systems and from reputable providers and/or issuing institutions;
- in the event of the introduction into the economic circuit of non-cash payment instruments that are obviously forged and/or altered, or even simply suspected of being forged, notify the competent authorities.

3.10. Environmental Crimes (Article 25-*undecies* of the DECREE)

In accordance with Article 6 of the DECREE, the following operations exposed to risk during whose performance or implementation the crimes under Article 25-*terdecies* of the DECREE may be committed, are identified in the COMPANY:

- use of substances or products subject to specific regulations and management of compliance in accordance with the provisions of the law;
- relations with public organisations in the event of audits, inspections and relevant compliance;
- management of products, completion of control logs and information flows to supervisory authorities;
- management of relations with public bodies for obtaining or renewing authorisations, licences, certificates, permits and concessions for conducting business activities and for the manufacturing plant, as well as for the management of approval, certification and declaration of conformity practices by the relevant authorities and institutes, also during audits;
- preparation and transmission of the documentation necessary to obtain authorisations, licences, permits, certificates and concessions;
- management of requirements, checks and inspections relating to: the use of hazardous substances; waste production and disposal; discharge into water and atmospheric emissions;
- activities in compliance with the provisions on the control of major-accident hazards and the requirements of the Single Environmental Authorisation (AUA – Autorizzazione Unica Ambientale);
- relations with public organisations during audits, inspections and compliance related to waste disposal and environmental management, as well as preparation and transmission of relevant documentation.

3.10.1. Principles underlying the procedures

Compliance with environmental protection regulations and adaptation of technical solutions

The Legal Department and the other functions concerned plan compliance audits in relation to regulatory and technical-scientific developments in environmental protection.

A so-called "environmental vendor list" is drawn up, specifying the suppliers and consultants that the COMPANY has assessed as suitable for the identification and implementation of controls.

Planning of environmental protection oversight

A budget, annual and long-term investment plans and specific programmes are drawn up in order to identify and allocate the resources needed to achieve environmental protection targets.

Every decision is based on the principle that the best environmental protection prevails over time and cost savings.

Traceability and separation of the phases of the procedure for the identification and implementation of the oversight is foreseen.

Procedures are formalised to regulate relations with the Public Administration organisations responsible for issuing authorisations and certifications in environmental matters or for carrying out inspections and checks.

A specific procedure is in place for the management of environmental emergencies.

Monitoring of environmental protection oversight

A procedure for the systematic monitoring of environmental protection data and indicators is in place and envisages:

- roles and responsibilities;

- the definition of specific performance indicators of environmental protection measures to assess their effectiveness and efficiency;
- monitoring activities;
- the introduction of corrective actions for any system shortcomings.

The procedure must provide for: the detection, recording and investigation of actual accidents and near-misses and of potentially harmful situations, the measures taken and reporting to the competent authorities. Declarations and certifications submitted are checked to ensure that they correspond to the supporting technical documentation.

Roles, responsibilities and procedures for periodic reporting to the Managing Director and the COMMITTEE on activities to assess the effectiveness and adequacy of the controls are identified.

Environmental protection audits

The following are identified:

- the scope, frequency, methodology, competencies, roles, responsibilities and requirements for the conduct of audit activities;
- the recording and communication of the results of the application of technical and organisational solutions for the management and control of operational aspects, according to legal and company requirements;
- systematic checks on the state of implementation of the measures adopted to neutralise the risk of environmental offences being committed;
- corrective actions in the event of departures from technical and organisational requirements;
- verification of the implementation and effectiveness of the actions taken.

Engagement and training of personnel in environmental protection

The following must be envisaged:

- regular meetings with management, workers and their representatives to raise awareness of environmental protection issues;
- training and updating activities, including hands-on drills, with management, workers and their representatives;
- specific training programmes that take into account any accidents with consequences for the environment.

Selection and monitoring of suppliers in environmental protection

In the selection of waste collectors, disposers, intermediaries and transporters, checks are made on the existence of valid registrations, communications and authorisations required by waste management regulations.

Checks are carried out on: the technical and professional suitability and authorisations of third parties carrying out activities that are relevant from an environmental point of view; the performance of suppliers with regard to compliance with environmental regulations.

Identification of specific oversight for areas particularly exposed to risk

A. FIRE

1. *Safety of wiring and fire-fighting systems*

Special procedures are envisaged to oversee:

- requests for the certificate of conformity of the work and correct installation;
- filing of the original documentation;
- the delivery of the certificate to the fire brigade when renewing the fire safety certificate (CPI);
- periodic inspections of the notifying bodies.

2. *Prevention*

The following requests are regulated:

- opinion of conformity for fire prevention for new installations;

- issue of the plant's CPI, accompanied by sworn appraisal and the "nothing has changed" declaration;
- inspection and update of the CPI.

The fire prevention register and periodic checks of the detection systems and extinguishing equipment are established.

B. WASTE

Management of the waste register and annual reporting of production and disposal

Procedures are formulated to regulate the:

- periodic authorisation to deposit special hazardous waste;
- keeping the loading and unloading logs, including the obligation to register and keep records in their original form in the National Electronic Register for Waste Traceability (RENTRI), as well as the transmission of recorded data via the RENTRI portal.
- management of the processes of waste delivery to authorised disposal companies;
- completion of eco-forms;
- approval of waste;
- shipment and control of delivery;
- verification of disposal;
- annual environmental declarations form (MUD);
- identification and EWC coding of new waste;
- ten-year archiving of documentation;
- waste management and traceability.

C. ENVIRONMENTAL REMEDIATION AND RESTORATION

Safety, environmental remediation and restoration of polluted sites

Specific procedures are in place to regulate:

- classification of the site;

- the project to make the implementation system safe;
- the provisional and definitive remediation and implementation project;
- periodic verification of the condition of the site;
- wastewater treatment;
- periodic analytical monitoring of the effectiveness of the treatment;
- declaration of completion of remediation and communication to the authorities.

D. SPECIAL EQUIPMENT

1. *Management of pressure equipment*

Procedures are formalised and envisage:

- the purchase of machinery manufactured by certified suppliers that apply the European Pressure Equipment Directive;
- the need to provide the manufacturer with technical design data for the correct sizing of the machinery;
- the need to obtain the CE conformity certificate, the use and maintenance manual and the filing of the machine in the Italian National Institute of Occupational Safety and Prevention (ISPESL) booklet.

2. *Commissioning and use of pressure equipment – implementation of the pressure equipment directive (PED)*

Procedures are in place to regulate:

- the request to ISPESL for the first plant inspection of new machinery;
- filing of documents on the machines and the checks carried out;
- management of the safety valves;
- PED requalification of pipes installed before 2000 and with a diameter greater than 80 DN;
- certification of new and installed pipes replacing the previous ones.

E. DISCHARGES, EMISSIONS, HAZARDOUS SUBSTANCES AND PRODUCTS

Special procedures are envisaged to regulate:

- authorisations for water discharge, atmospheric emissions and fluid storage;
- periodic analyses of discharge and emissions;
- management of assets containing ozone depleting substances;
- communications to the regional environmental agency (ARPA);
- registration and management of chemical substances and compliance with current regulations;
- labelling according to European regulations and the correct transport of hazardous goods;
- updating of the classification of substances and safety data sheets.

3.11. Tax Crimes (Article 25-*quinquesdecies* of the DECREE)

In accordance with Article 6 of the DECREE, the operations exposed to risk during whose performance or implementation the crimes under Article 25-*quinquiesdecies* of the DECREE may be committed, are identified as follows:

- tax-related obligations;
- purchase of goods and services;
- purchase and sale of company assets;
- distribution and sales to customers;
- organisation of conferences and sponsorship of conferences organised by third parties;
- donations, grants and other charitable initiatives;
- relations with bank intermediaries;
- cash flow management;
- application for public funding and grants and management thereof;
- acquisition and management of software licences;

- preparation of financial statements, reports and communications;
- management of dealings with independent auditing firms and the board of statutory auditors;
- intercompany transactions;
- management of extraordinary transactions;
- management of expenses claims;
- training supported by funding.

3.11.1. Principles underlying the procedures

In addition to the principles already listed on the management of financial resources and on the recording and verification of the correctness of the accounting transactions, the following principles are envisaged:

Tax-related obligations

Tax obligations are discharged in accordance with the due dates and procedures established by the tax authorities and the relevant legislation.

The operating and control methods for carrying out the various stages of the procedure are formally defined, after identifying the competent corporate functions and the relevant duties assigned to them.

Functions are kept separate by spreading them amongst the persons who calculate the taxes, those who check their accuracy and those who authorise payment or transmission. Measures are taken to ensure that tax returns are prepared in accordance with the principles of truthfulness, completeness and transparency.

The data and information contained in the tax returns are audited for accuracy, completeness and correspondence with the accounting records.

Tax returns are prepared and signed by the formally identified person with appropriate powers.

An external consultant calculates direct taxes under the supervision of the GROUP's Tax function and the calculation is shared with the Director of Administration and Finance.

The relevant functions check the final tax calculation after approval of the financial statements.

The relevant records are archived with the competent Departments.

Assignment of positions and advisory services, purchase of goods and services, and sales to customers

Before archiving tax records, periodic second-level checks are carried out on the completeness and correspondence to payment transactions of documents relating to the company's receivables and payables. The Human Resources Department is involved in appointing scientific consultants in order to apply the correct tax treatment.

In the pursuit of the principle of separating functions, before assigning the appointment, the following assessments must be carried out *(i)* the adequacy of the amount and the absence of any conflict of interest (Responsible Department); *(ii)* scientific nature of the consultancy (Medical and Scientific Department); and *(iii)* compliance of the initiative with applicable laws and regulations, as well as the appropriateness of the expenditure (Pharma Compliance).

Payment of the amount due is subject to prior verification of the performance of the service through the acquisition of specific evidence; of the adequacy, also of the amounts specified in the invoice, with respect to the contract signed.

Organisation and sponsorship of conferences and events

Each initiative undergoes a preliminary control procedure, guided by the principle of separation of duties, as follows: *(i)* the Marketing Manager verifies compliance with the Farmindustria Code of Ethics; *(ii)* the Medical-Scientific Director ensures the relevance of the subject addressed with the pharmacological product of reference; *(iii)* lastly, the Pharma Compliance Department ascertains the economic adequacy of the sponsorship expenses incurred by the COMPANY and statutory compliance.

For the purposes of the correct application of tax regulations, it is necessary to verify the following: the actual sponsorship by collecting documentary proof; correspondence of the

actual amount with the budget estimate approved by the Italian Ministry of Health. Anything in excess cannot be considered a tax deductible.

Cash flow management

Specific procedures are in place to regulate the:

- persons responsible, the procedures and the controls put in place to monitor the stages of the process;
- traceability of the phases relating to the management of collecting payments;
- methods of managing cash flows that do not fall within the scope of ordinary business processes and are of an exceptional and urgent nature;
- methods of filing the records supporting the collection operations.

It is forbidden to make or receive payments on numbered accounts; likewise, payments may not be accepted from persons holding current accounts registered in "tax havens" or in countries belonging to the so-called "black list" and "grey list", unless this is their country of residence or the country where the service was provided. With reference to financial receivables, before proceeding with electronic archiving of the records, a second-level check that records are complete is performed.

Management of public funding and grants

The functions involved in preparing projects for funding activities of corporate interest must ensure the truthfulness and completeness of the information provided.

Consultants and external counterparts which the COMPANY uses to obtain public funding and grants are monitored.

At each stage of the progress of projects, ITALFARMACO provides the financing body with the scientific, administrative and accounting documentation confirming the activities carried out, including the statement of costs.

All records relating to the process are duly archived.

Intercompany dealings

Intercompany contracts are signed and performed in compliance with a specific procedure that establishes the:

- roles, responsibilities, and rules of conduct to be observed and the operating and control procedures for each stage of the process;
- traceability of the various stages, in particular with respect to the definition of contractual agreements, the production of documentary evidence to support the chargeback of costs to subsidiaries and the sharing of data on costs;
- procedures for archiving relevant records.

Before proceeding with the preparation of the contract, a written opinion on the tax profiles must be obtained from the Tax Manager, in order to identify any critical issues and identify the methods for calculating the amount to charge the intercompany organisations, defining in particular the criteria and methods of chargeback.

Extraordinary transactions

A specific procedure identifies the persons responsible, the system of controls and the procedures for obtaining opinions on tax treatment.

Transactions must be adequately backed up with documentary evidence.

Appropriate due diligence is always performed on the extraordinary transaction, after the preliminary checks carried out by the relevant Functions and before the initiative is submitted to the COMPANY'S Board of Directors.

Electronic or hard copy records must be archived.

Management of expenses claims

The procedure for submitting expense claims is regulated according to the type of personnel involved, belonging to the external or head office network, as the case may be.

Expenses claims must be accompanied by *(i)* adequate documentary evidence, and *(ii)* the tax records required by the relevant legislation.

The competent functions must make sure that the documentary evidence attached corresponds to the content of the expense claims.

The records are archived with the competent Departments.

Training supported by funding

Training activities must be adequately justified and traceable.

Procedures are in place for the electronic archiving of documents relating to the planning, execution and reporting of activities.

3.12 Smuggling (Article 25-*sexiesdecies* of the DECREE)

Pursuant to Article 6 of the DECREE, the operations exposed to risk, during the performance or execution of which, the crimes under Article 25-*sexiesdecies* of the DECREE may be committed are as follows: management of relations with the Customs Authorities for import and export of raw materials, semi-finished and finished products.

3.12.1. Principles underlying the procedures

Procedures are formally established to identify the roles, responsibilities, operating and control methods relating to the following activities:

- *importation* - supplier checks, approval of orders, management and control of customs clearance, as well as the conformity assessment of the item received;
- *exportation* - customer controls, the definition of trade agreements, activities preparing for shipment, verification of correct customs clearance and export conformity, management of credit notes and returns;
- *three-way trade*, listing the documents which must be acquired.

Functions are kept separate by breaking the activities down to *(i)* executive, performed by the Exports function; *(ii)* control under the responsibility of the Finance & Accounting function, and *(iii)* authorisation, the remit of the Head of Alliance Management and the Site Head.

The records – analytically identified by the COMPANY procedures – are archived with the relevant functions.

3.13 Crimes against animals (art. 25-*undevicies* of the Decree)

- Pursuant to Article 6 of the DECREE, the following are identified as risky operations in the performance or execution of which the offences referred to in Article 25-undevicies of the DECREE may be committed:preclinical research activities;
- clinical trials, including non-profit trials;
- activities related to the production of medicines;
- purchase of goods and services

3.13.1. Guiding principles of the procedures

It is forbidden to engage in, collaborate in or cause the implementation of conduct which, taken individually or collectively, directly or indirectly constitutes the offences against animals referred to in Article 25-undevicies of Legislative Decree 231/2001

Preclinical research; clinical trials, including non profit trials; activities related to the production of medicinesThose involved in the above activities are also prohibited from:

- voluntarily causing the death of an animal out of cruelty or without necessity;
- inflict severe suffering through sheer brutality;
- neglecting to treat a condition, leading to its worsening and significant suffering;
- causing injury or subjecting the animal to cruelty, fatigue or treatment incompatible with the ethological characteristics of the species
- administering narcotic and/or prohibited substances
- carry out treatments that are harmful to the health or physical integrity of the animal;

- administer unauthorised vaccines;
- rendering another person's animal unusable or causing it to deteriorate without necessity or objective justification.

Furthermore, it is mandatory to:

- ensure that animals are kept in healthy, clean and adequately sized environments;
- Avoid training methods based on painful or coercive stimuli (e.g. electric collars);
- avoid imposing behaviours that are incompatible with the typical behaviour of the species;
- ensure transport in suitable conditions with sufficient ventilation;
- ensure the diligent care of the animal entrusted to you for any reason;
- take prompt action in the event of illness.

In any case, compliance with special regulations on scientific experimentation, pursuant to Legislative Decree 26/2014.

The competent departments are responsible for verifying compliance with the above prohibitions and monitoring the conduct of internal and external parties involved..

Purchase of goods and services

It is expressly prohibited to assign supply contracts to third parties if there is any evidence, even circumstantial, of a violation of regulations or ethical principles regarding animal welfare.

Finally, documentation proving regulatory compliance, activity tracking and any control system implemented must be stored electronically or in paper form.

Annexes:

All.01 EXAMINATION OF THE OFFENCES

All.02: Code of Ethics

All.03: Whistleblowing Procedure