Organisation, management and control model under Legislative Decree 231/2001

GENERAL PART

VERSION NO.	DATE	NOTES
01	**31 May 2023**	First issue
02	**July 2023**	Second issue
03	**12 April 2024**	Third issue
04	**June 2026**	Fourth issue

DEFINITIONS 5

CHAPTER 1: THE ADMINISTRATIVE LIABILITY REGIME OF LEGAL PERSONS, COMPANIES AND ASSOCIATIONS 8

1.1 Legislative Decree 231/2001 and the relevant legislation 8

1.1.1 Liability under Legislative Decree 231/2001 8

1.1.2 Offences 9

1.1.3 Applicability of Legislative Decree 231/2001 to foreign-law entities 11

1.2 The adoption of the 'organisation, management and control model' as a possible exemption from administrative liability 12

CHAPTER 2: THE COMPANY, THE GROUP, GOVERNANCE AND ORGANISATIONAL STRUCTURE 14

2.1 The Company 14

2.2 The organisational structure of the Company 14

2.2.1 Shareholders' Meeting 14

2.2.2 Board of Directors 15

2.2.3 Board of Auditors 15

2.2.4 Organisation 15

CHAPTER 3: ADOPTION OF THE MODEL 17

3.1 Objectives pursued with the adoption of the Model 17

3.2 Scope of the Model 18

3.3 Underpinning elements and principles of the Model 18

3.4 Adoption of the Model 19

3.5 The 'acceptable risk' approach 19

3.6 Model Structure 20

3.7 Criteria for preparing the Model 20

3.7.1 Phases 20

3.7.2 Methodology adopted to prepare the Special Part of the Model 22

3.8 Addressees of the Model 22

CHAPTER 4: THE SUPERVISORY BODY 23

4.1 Appointment of the Supervisory Body 23

4.2 Eligibility Requirements 23

4.2.1 Strengthened autonomy and independence 23

4.2.2 Honourability and grounds for ineligibility 25

4.2.3 Proven professionalism, specific skills in inspection and consultancy work 26

4.2.4 Continuity of action 26

4.3 Term of office 26

4.4 Function of the Supervisory Body 27

4.5 Powers of the Supervisory Body 30

4.6 Rules of convocation and operation 31

4.7 Reporting by the Supervisory Body 31

4.8 Information flows to the Supervisory Body 32

4.9 Reports of conduct relevant to the Model 34

4.10 Confidentiality obligations 35

4.11 Collection and storage of information 35

CHAPTER 5: DISSEMINATION AND TRAINING 36

5.1 Dissemination 36

5.2 Training 36

CHAPTER 6: THE DISCIPLINARY SYSTEM 38

6.1 Function of the Disciplinary System 38

6.2 Relevant conduct 38

6.3 Penalties 39

6.4 Measures against directors and attorneys 40

6.5 Measures against auditors 40

6.6 Measures against Third Parties 41

CHAPTER 7: CHECKS ON THE MODEL's ADEQUACY 42

CHAPTER 8: THE COMPONENTS OF THE MODEL 43

8.1 The Elements of the Model 43

8.2 Organisational Elements of the Model 43

8.3 The general controls..... 43

8.3.1 The Code of Conduct 43

8.3.2 The Anti-Bribery Policy 44

8.3.3 System of powers 44

8.3.4 Segregation 45

8.3.5 Traceability and archiving 45

8.3.6 Management system for outsourced processes 45

8.3.7 Cash flow management and control system 46

8.3.8 Checks and monitoring 47

8.3.9 Information flows 47

8.3.10 Contractual clauses 47

8.4 Control Protocols of the Special Part..... 47

DEFINITIONS

- "Sensitive Activities": activities carried out by the Company that are exposed to the risk of commission of Offences.
- "Board of Directors" or "Board": the Company's board of directors.
- "Chiesi": Chiesi farmaceutici S.p.A.
- "Contributors": those who act in the name of and/or on behalf of UNIKERIS under a mandate, or those who collaborate with UNIKERIS under a collaboration agreement of any nature (excl. Consultants and Partners).
- "Code of Conduct": the Code of Conduct adopted by Chiesi Farmaceutici S.p.A. and valid for the entire Group
- "Consultants" means any natural person or independent company working on behalf of UNIKERIS and/or a Group company to provide expert advice or professional services of an intellectual nature to be used by UNIKERIS and/or a Group company.
- "Addressees": the parties indicated in clause 3.8 of this Model.
- "Legislative Decree 231/2001" or "Decree": Legislative Decree No. 231 of 8 June 2001 and subsequent amendments and additions.
- "Suppliers": the Company's suppliers of professional and non-professional goods and services, including those of a financial nature.
- "Function(s)": all company and/or Group functions assigned to the performance of company activities relevant to this Model.
- "Group" or "Chiesi Group": Chiesi Farmaceutici S.p.A. and all its subsidiaries.
- "Confindustria Guidelines": the guidelines for the construction of organisation, management and control models under Legislative Decree 231/2001 approved by Confindustria, in the latest version published in June 2021.
- "Management": the members of the Board of Directors, the heads of secondary offices and the heads of the main Group Functions involved in Sensitive Activities.
- "Model" or "231 Model": the organisation, management and control model stipulated under Legislative Decree 231/2001.

- "Corporate Bodies": the Board of Directors and the Board of Auditors of the Company.

- "Supervisory Body" or "Body" or "SB": internal body (single member or multiple member) responsible for supervising the operation of and compliance with the Model and its updates.

- "P.A." or "Public Administration": public administrative bodies, including its officials and individuals in charge of public services, such as: the judicial authorities; Italian and foreign national and local institutions and public administrative bodies; the Antitrust Authority; the Italian Medicines Agency ("**AIFA**"); the Italian Data Protection Authority; the Authority for Electricity, Gas and the Water System; and other Italian and foreign supervisory authorities, or private entities with equivalent functions, and their relevant officials and internal bodies.

- "Partners": contractual counterparties of the Company, both natural and legal persons, with whom the Company enters into any form of contractually regulated cooperation relationship whereby they cooperate with the Company in the context of Sensitive Activities.

- "Anti-Bribery Policy": the Anti-Bribery Policy of the Chiesi Group, formally adopted by UNIKERIS by a resolution of the Board of Directors on 5 December 2022.

- "Company procedures": policies, guidelines, operating instructions, company and/or Group SOPs relevant to the performance of Sensitive Activities.

- "Processes": company areas of Sensitive Activities.

- "Product": the pharmaceutical product distributed by the Company – also through other Group companies – to prevent, cure and treat rare diseases and pathologies.

- "Control Protocols": the rules of conduct, prohibitions and controls aimed at preventing, with regard to each Process, the commission of the Offences.
- "Public Officials": (a) any person exercising a legislative, judicial or administrative public function; (b) any person acting in an official capacity in the name of or on behalf of: (i) a Public Administration of a State, whether local, national or federal; (ii) an agency, office or body of the European Union or of a Public Administration of a State; (iii) where the law of the relevant State so provides, an enterprise owned, controlled or participated in by a Public Administration of a State, unless this enterprise operates on a normal

commercial basis in the relevant market, i.e., on a basis substantially equivalent to that of a private enterprise; (iv) a public international organisation, such as the European Bank for Reconstruction and Development, the International Bank for Reconstruction and Development, the International Monetary Fund, the World Bank, the United Nations or the World Trade Organisation; or (v) a political party, a member of a political party or a candidate for political office, whether Italian or foreign; or (c) any person in charge of a public service, to be understood as a person who, for whatever reason, performs a public service (i.e., an activity that is regulated in the same manner as a public function, but characterised by a lack of powers typical of a public function). The performance of simple orderly tasks and the performance of merely material work are excluded.

- "Offence(s)" or "Predicate Offence(s)": any of the offences referred to in Legislative Decree 231/2001.

- "System of Powers": the set of proxies and powers of attorney granted within the Company, as well as any powers of representation granted to Third Parties.

- "Disciplinary System": the disciplinary system forming part of this Model.

- "SpeakUp&BeHeard": the Chiesi Group's reporting system consisting of a dedicated platform (independent of the Company's information systems) and a voicemail.

- "Third Parties": independent third parties who perform their activities by supplying goods and/or providing services in the interest/advantage and/or in the name and on behalf of the Company in relation to the Sensitive Activities regulated by this Model. Third Parties also include Consultants, Contractors, Suppliers, any intermediaries and/or agents and Partners who perform their activities in the interest/benefit and/or in the name and on behalf of the Company and in relation to any Sensitive Activities.

- "UNIKERIS" or "Company": UNIKERIS LIMITED, with registered office in Manchester M22 5LG (United Kingdom), 333 Styal Road and with secondary office in Parma (PR), Stradello Marche 6.

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

1.1 Legislative Decree 231/2001 and the relevant legislation

1.1.1 Liability under Legislative Decree 231/2001

Legislative Decree No. 231 of 8 June 2001 ("**231 Decree**") entered into force on 4 July 2001 and sets out the "regulations on the administrative liability of legal persons, companies and associations, including those without legal personality".

The Decree aimed to bring domestic legislation governing the liability of legal persons into line with several international conventions to which Italy had long since acceded, such as the Brussels Convention of 26 July 1995 on the protection of the financial interests of the European Communities, the Brussels Convention of 26 May 1997 on combating bribery involving officials of the European Community or its Member States, and the OECD Convention of 17 December 1997 on combating bribery of foreign public officials in international and economic transactions.

Art. 5 of Legislative Decree 231/2001 sets out the liability of a company if specific offences (i.e., predicate offences) are committed in its interest or to its advantage:

(a) by '**apical**' persons, i.e., persons who: (i) hold positions of representation, administration or management of a company or of an organisational unit of a company with financial and functional autonomy; or (ii) exercise, even de facto, the management and control of a company (e.g., directors and general managers); or

(b) by persons "subject to the **direction or supervision**" of any apical person indicated in point (a) above (i.e., all non-managerial employees and Third Parties).

Therefore, if any predicate offences are committed by the above persons, the criminal liability of a natural person who materially committed the offence is added – if and insofar as all the other regulatory prerequisites are met – to the 'administrative' liability of the company.

These rules therefore aim to include corporate entities among parties subject to criminal penalties for specific offences that are committed in their interest (with a view to the corporate policy adopted) or to their advantage (to obtain a pecuniary benefit from the commission of the offence)[6] With regard to criminal penalties, all offences committed always

[6] Recent guidelines of the Supreme Court of Cassation – also referred to by the Confindustria Guidelines – show that in culpable offences (health & safety offences and environmental offences) the interest or advantage must also refer to a breach of precautionary rules (e.g., saving safety costs; increasing performance speed or productivity; or sacrificing the adoption of accident prevention measures).

entail the application of a pecuniary penalty against the legal person; for more serious offences, the application of prohibitory penalties is also envisaged, such as disqualification from carrying on a business; suspension or revocation of authorisations, licences or concessions; prohibition from contracting with the Public Administration; exclusion from financing, contributions or subsidies and the possible revocation of those already granted; and prohibition from advertising goods and services.

The liability imposed by the Decree also arises in relation to offences committed abroad if the State in which the offence was committed does not prosecute the specific offence.

Additionally, any incriminating offences listed under the Decree that are attempted result in the company incurring liability under the Decree. More specifically, Art. 26(1) of the Decree envisages that, in cases where the indicated offences are attempted, the pecuniary penalties (in terms of amount) and disqualification penalties (in terms of time) are reduced by between one third and one half. However, under Art. 26 of the Decree, a company is excluded from liability for attempted offences if it "voluntarily prevents the action from being carried out or the event from taking place".

1.1.2 Offences

The typology of predicate offences is very broad and includes the following offences:

(a) undue receipt of funds; fraud to the detriment of the State, a public body or the European Union or for the purpose of obtaining public funds; computer fraud to the detriment of the State or a public body; and fraud in public procurement (Art. 24 of Legislative Decree 231/2001);

(b) computer crimes and unlawful processing of data (Art. 24-*bis* of Legislative Decree 231/2001);

(c) organised crime offences (Article 24-*ter* of Legislative Decree 231/2001);[7]

(d) embezzlement, extortion, undue induction to give or promise benefits, bribery and abuse of office (Art. 25 of Legislative Decree 231/2001);

(e) offences of counterfeiting money, public credit cards, revenue stamps and identification instruments or signs (Art. 25-*bis* of Legislative Decree 231/2001);

[7] The Company adheres to the interpretative orientation on the identification of the predicate offence for the offence of criminal conspiracy, whereby 231 liability of the entity for the offences set out in Legislative Decree 231/2001 must be limited solely to cases in which the contested case is included in one of the Predicate Offences indicated in the Decree itself (see Criminal Court of Cassation, Section VI, no. 3635 of 24 January 2014). The Company also adopts this approach in relation to the assessment of the offence of self-money laundering, in line with the criteria clarified by the Confindustria Guidelines on this point.

(f) offences against industry and trade (Art. 25-*bis*.1 of Legislative Decree 231/2001);

(g) corporate offences (Art. 25-*ter* of Legislative Decree 231/2001);

(h) offences with the purpose of terrorism or subversion of the democratic order (Art. 25-*quater* of Legislative Decree 231/2001);

(i) offences relating to female genital mutilation practices (Art. 25-*quater*.1 of Legislative Decree 231/2001);

(j) offences against the individual (Art. 25-*quinquies* of Legislative Decree 231/2001);

(k) market abuse crimes and administrative offences (Art. 25-*sexies* of Legislative Decree 231/2001);

(l) transnational offences (Art. 10 of Law No. 146 of 16 March 2006);

(m) offences of culpable homicide and grievous or very grievous bodily harm committed in breach of the rules on the protection of health & safety at work (Art. 25-*septies* of Legislative Decree 231/2001);

(n) offences of receiving, laundering and using money, goods or benefits of unlawful origin, as well as self-money laundering (Art. 25-*octies* of Legislative Decree 231/2001);

(o) offences relating to non-cash means of payment (Art. 25-*g*.1 of Legislative Decree 231/2001);

(p) copyright infringement offences (Art. 25-*novies* of Legislative Decree 231/2001);

(q) inducement not to make statements or to make false statements to the judicial authorities (Art. 25-*i* of Legislative Decree 231/2001);

(r) environmental offences (Article 25-*undecies* of Legislative Decree 231/2001);

(s) employment of third-country nationals whose stay is irregular (Art. 25-*duodecies* of Legislative Decree 231/2001);

(t) crimes of racism and xenophobia (Art. 25-*terdecies* of Legislative Decree 231/2001);

(u) fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited apparatus (Art. 25-*quaterdecies* of Legislative Decree 231/2001);

(v) tax offences (Art. 25-*quinquiesdecies* of Legislative Decree 231/2001);

(w) smuggling offences (Art. 25-*sexiesdecies* of Legislative Decree 231/2001);

(x) cultural heritage offences (Art. 25-*septiesdecies* of Legislative Decree 231/2001); and

(y) laundering of cultural goods and devastation and looting of cultural and landscape goods (Art. 25-*duodevicies* of Legislative Decree 231/2001);

(z) offences against animals (Art. 25-*undevicies* of Legislative Decree 231/2001).

However, **not all the Presumed Offences are currently conceivable** in relation to the Company's business activities. The **Special Part of the Model** indicates which specific Crimes are considered potentially relevant in the performance of the Company's activities.

1.1.3 Applicability of Legislative Decree 231/2001 to foreign-law entities

Art. 1(2) of Legislative Decree 231/2001 defines the scope of application of the rules governing the administrative liability of entities without drawing any distinction between entities established in Italy and entities established abroad.

From the outset, the jurisprudence on its merits has expressed the view that because the criterion that establishes jurisdiction to decide on an entity's administrative liability (i.e., under Art. 36(1) of Legislative Decree No. 231/2001) applies the legal rule of *locus commissi delicti* (i.e., the place where the predicate offence was committed), a legal entity whose head office is abroad can be investigated if the predicate offence was committed in Italy.

Also, according to recent caselaw,[8] there is "no reason to believe that legal persons are subject to special rules compared to those in force for natural persons so as to escape the principles of the mandatory nature and territoriality of criminal law". In fact, Arts. 3 and 6(1) of the Criminal Code stipulate that: (a) Italian criminal law is mandatory against all persons on Italian territory, irrespective of their nationality, subject to the exceptions of public and international law; and (b) an offence committed on Italian territory can be prosecuted under Italian law.

Therefore, full or partial commission of an Offence on Italian territory entails Legislative Decree 231/2001 being applied to the entity in whose interest or to whose advantage the Offence was committed, regardless of whether the entity has its head office in another country or whether the law of that country does not provide for organisational-preventive burdens similar to those of Legislative Decree 231/2001.

[8] *See Criminal Court of Cassation,* sect. VI, decision no. 11626 of 7 April 2020 (in accordance with Criminal Court of Cassation, sect. IV, judgment no. 32899 of 8 January 2021 - dep. 6 September 2021).

1.2 The adoption of the 'organisation, management and control model' as a possible exemption from administrative liability

Art. 6 of the Decree introduces a special form of exemption from the liability in question if the company proves that:

(a) it has adopted and effectively implemented through its management body, before the commission of the offence, an organisational and control model capable of preventing offences of the kind committed;

(b) it has entrusted an internal body with autonomous decision-making and control powers with the task of supervising the operation of and compliance with the model, as well as ensuring that it is updated;

(c) the persons who committed the offence acted by fraudulently evading the above model; and

(d) there has been no or insufficient supervision by the body referred to in point (b) above.

The Decree (as amended by Legislative Decree No. 24/2023[9]) also envisages that the organisation and control model – in relation to the extent of the delegated powers and the risk of commission of the Offences – must meet the following requirements:

1. identify all activities whose scope entails a risk of Offences being committed (i.e., Sensitive Activities);
2. set out, or refer to, specific protocols governing the formation and implementation of corporate decisions in relation to the Offences to be prevented;
3. identify the financial resources suitable for implementing an organisational system to prevent the commission of the Offences;
4. impose information obligations towards the body that supervises the functioning of and compliance with the model;
5. set up an internal disciplinary system capable of penalising non-compliance with the measures indicated in the model;
6. establish internal reporting channels and prohibition of retaliatory actions according to Legislative Decree No. 24/2023 ("**Decree 24/23**");

[9] Legislative Decree No. 24/2023 "*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council dated 23 October 2019 on the protection of persons who report breaches of Union law and bearing provisions concerning the protection of persons who report breaches of national laws*".

7. provide within the disciplinary system mentioned under point 5 above specific penalties against whoever (i) breaches the confidentiality protection measures set out by article 12 of Decree 24/23 for the whistleblower, the persons involved and persons mentioned in the reported conduct; (ii) adopts retaliatory actions against the whistleblower (and/or the further persons/entities reported under article 3.5 of Decree 24/23[10]), for reasons connected, directly or indirectly, to the report made; (iii) hampered or attempted to hamper report submission.

CHAPTER 2: THE COMPANY, THE GROUP, GOVERNANCE AND ORGANISATIONAL STRUCTURE

2.1 The Company

UNIKERIS LIMITED is a company incorporated under English law with its registered office in Manchester M22 5LG (United Kingdom), 333 Styal Road and its own Italian branch office in Parma (PR), Stradello Marche 6, as of 1 January 2022. The Company is tax resident in Italy.

The Company's main activity is the Product's distribution. Currently, the Company distributes, through Group companies or third parties (incl. Partners and Third Parties), the Product to hospital institutions in different geographic areas (e.g., Europe, Turkey, Middle East and Japan). The Product is licensed in the USA and Japan.

2.2 The organisational structure of the Company

The Company's share capital is represented by shares wholly owned by Chiesi Farmaceutici S.p.A., which is therefore the Company's sole shareholder.

The Company's legal form is a single-member private company limited by shares and its governance system consists of Shareholders' Meetings, a Board of Directors and a Board of Statutory Auditors.

2.2.1 Shareholders' Meeting

Resolutions passed by a Shareholders' Meeting are either ordinary or extraordinary in accordance with applicable law. More specifically, ordinary resolutions must be passed for:

[10] According to article 3.5 of Decree 24/23, protection measures against the retaliatory actions reported under article 17 of Decree 24/23 apply to: whistleblowers (i.e. persons both internal and external to the company and linked to it by an employment and/or collaboration relationship, as defined under article 3 of Decree 24/23); whistleblower's facilitators; persons in the same work environment as the whistleblower and who are related to him/her by a stable emotional bond or kinship within the fourth degree; colleagues of the whistleblower, who work in the same work environment as the whistleblower and who have a usual and running relationship with the same; entities owned by the whistleblower or for which the same whistleblower works, as well as to entities operating in the same work environment of the whistleblower.

approvals of the Company's annual financial statements; appointments and dismissals of directors; appointments of the Board of Statutory Auditors, its Chairman and any person or entity entrusted with the legal auditing of the Company's accounts; setting directors' and auditors' remuneration; and any resolutions on the liability of directors and auditors. Amendments to the Articles of Association, the dissolution of the Company, the appointment of liquidators and any other matters under the law or the Articles of Association must be approved by special resolution.

The Assembly is chaired by the Chairman of the Board of Directors.

2.2.2 Board of Directors

The Board of Directors is entrusted with the Company's management and to this end it performs all acts and transactions regarding the Company's ordinary and extraordinary administration, excl. acts and transactions that the law or the articles of association expressly reserve to the shareholders.

Currently, the Board of Directors takes the form of a five-member board of directors, with an Italian majority. Additionally, the board of directors appoints three members of the Board of Directors as '*institori*' with powers over management of the Company's branch office under Arts. 2203 to 2208 inclusive of the Italian Civil Code. These powers are to be exercised severally and with the power to sub-delegate individual acts or categories of acts to third parties.

The Company's legal representation vests in the Chairman of the Board of Directors and also the members of the Board of Directors *(institori)* within the limits of the powers set out in the deed of appointment.

If powers are delegated to several directors, with joint and/or several powers, the legal representation also vests in them, consistently with the delegated powers.

2.2.3 Board of Auditors

The Board of Statutory Auditors is responsible for ensuring that: (a) the board of directors and shareholders meetings comply with the law and the articles of association; and (b) the principles of proper administration and the adequacy of the organisational, administrative and accounting structure are observed.

The Board of Statutory Auditors may: (a) carry out inspections and controls; and (b) request information from the directors regarding the company's management or specific business matters.

2.2.4 Organisation

The Company is small; and all major management and business decisions relating to the Company's activities are taken in Italy.

Corporate activities are outsourced under specific contracts to: (a) third parties (incl. Third Parties); and (b) other Group companies (with the support of specific corporate functions).

With regard to outsourcing business activities under point (a) above, the Third Parties perform activities for the Company that include distribution of the Product, management and execution of orders for the Product, and participation in the procedures called by the Public Administration for the supply of the Product.

However, with regard to outsourcing of business activities under point (b) above, the Chiesi Group companies primarily involved are: (i) Chiesi Limited, which provides the Company with a range of services through functions/employees based in the UK (e.g., customer service, medical liaison services, medical affairs, management, financial services, consultancy and assistance for all matters relating to human resources management, legal services, company secretarial services, support services and regulatory and quality assurance services); and (ii) Chiesi Farmaceutici S.p.A., which provides management support services, tax compliance management for the secondary office and intellectual property services through functions/employees based in Italy.

The allocation of activities to Chiesi Farmaceutici S.p.A. makes it possible to make the Company's activities part of the broader Chiesi Group strategy and to standardize the management of the company's product portfolio and intellectual property rights.

CHAPTER 3: ADOPTION OF THE MODEL.

3.1 Objectives pursued with the adoption of the Model

The adoption of the Model was promoted in line with the Group's ethical and governance principles to ensure the appropriate conduct of all activities and prevent the commission of specific types of offences, i.e., those listed under the Decree.

The Company is aware of the value that can derive from an internal control system capable of preventing the commission of Offences by its Corporate Bodies and, in general, by third parties operating in the name of or on behalf of or in the interest of the Company, under the supervision of senior management. Also, the Company is aware that the adoption and effective implementation of the Model improves the system of Corporate Governance in that they limit the risk of the commission of Offences and allow it to benefit from the exemption under Legislative Decree 231/2001.

The Model has been prepared and implemented in the belief that beyond the Decree's provisions, which envisage the Model itself as an optional, non-mandatory element, the Model could constitute – in addition to an exempting circumstance under the Italian legislation on the liability of entities for administrative offences deriving from crime under Legislative Decree 231/2001 – a fundamental tool to raise awareness among all those who work in the name and on behalf of UNIKERIS. This will ensure that all those who work for the Company adopt the correct conduct when they perform their activities for the Company. The 231 Model serves as a fundamental instrument to raise awareness among all individuals who work in the name and on behalf of UNIKERIS to the need to adopt correct and honest conduct when performing their activities for the Company, which should therefore prevent the risk of commission of the Offences.

Therefore, the purpose of this Model is to set up a system of prevention, deterrence and control to reduce the risk of offences being committed by identifying the Sensitive Activities, the principles of conduct that must be complied with by the Recipients of the Model, and specific control activities, which are all aimed at preventing the commission of Offences.

More specifically, the Model aims to:

- develop an awareness among all those who work in the area of Sensitive Activities that – in the event of conduct that breaches the Model or other company rules and procedures (as well as with the law) – specific offences can have criminal consequences not only for themselves but also for the Company;

- reiterate that these forms of unlawful conduct are strongly condemned by the Company because (even if it were theoretically in a position to take advantage of them) they are in any case contrary not only to the law but also the Group's ethical and social principles; and
- enable the Company, by monitoring Sensitive Activities, to take timely action to prevent or counteract the commission of Offences.

3.2 Scope of the Model

The Model 231 covers all the activities carried out by the Company that are identified as potentially at risk of commission of the offences listed under the Decree (i.e., Sensitive Activities).

It is very important to emphasise that **the Model also covers Sensitive Activities that are wholly or partly entrusted to Third Parties or other Group companies**. The main Sensitive Activities wholly or partly entrusted to Third Parties or other Group companies are listed in the Special Part.

In this case, the individuals entrusted with these activities must also comply with all applicable provisions of this Model.

3.3 Underpinning elements and principles of the Model

The following are considered as cornerstones of the Model:

- Raising awareness of and disseminating the codes of conduct and procedures set at all levels of the company.
- Mapping Sensitive Activities.
- Risk prevention by adopting specific procedural principles aimed at regulating the formation and proper implementation of corporate decisions in relation to the Offences to be prevented.
- Control measures aimed at preventing the risk of offences being committed. More specifically, this includes the verification and documentation of all operations carried out in the context of Sensitive Activities; compliance with the principle of segregating roles when structuring corporate processes and managing financial resources; the definition of authorisation powers consistent with the responsibilities assigned; and the verification of corporate conduct. These control measures should result in the Model being periodically updated (i.e., ex post control).

- Giving the Supervisory Body specific tasks to supervise the effective and correct functioning of the Model.

More specifically, the Model **takes into account the existing and already operating company and Group control processes and systems** insofar as they are considered suitable to also serve as crime prevention and control measures on the processes involved in Sensitive Activities.

The 231 Model is characterised by: (a) effectiveness, i.e., the adequacy of the set of controls put in place to prevent the commission of alleged offences; (b) specificity, i.e., consideration of the Company's characteristics, size, business type and historical events; and (c) topicality, i.e., constant updating.

The Model's design has also been guided by a criterion of proportionality – within which rules and controls have been established that are proportionate to the small size and simplified organisational structure of the Company's secondary office – and the need for effective dissemination of the Model to all Addressees.

3.4 Adoption of the Model

This General Part of the Model was adopted for the first time on [31 May 2023] by a decision of the Board of Directors. This decision also appointed the Supervisory Body, which is entrusted with supervising the functioning, effectiveness and observance of the Model itself and promoting its updating.

3.5 The 'acceptable risk' approach

Essential in the construction of a preventive control system is the concept of '**acceptable risk**'. More specifically, for the purposes of applying Legislative Decree 231/2001, it is essential to determine an effective threshold that allows a limit to be placed on the quantity and quality of the preventive measures to be adopted and implemented to avoid the commission of the alleged offences. If the acceptable risk is not determined in advance, the quantity/quality of preventive controls that could be instituted would in fact be virtually infinite, with intuitable consequences in terms of company operations. The same general principle, which can also be invoked in criminal law, of the concrete enforceability of conduct constitutes a central reference criterion in this regard.

As pointed out by the Confindustria Guidelines on the appropriate preventive control system to build based on the risk of commission of the alleged offences, with regard to intentional offences, the acceptable threshold is met by deploying a prevention system that cannot be circumvented unless by fraud. This is in line with the logic of 'fraudulent evasion' of the 231

Model as an express exemption for the purposes of excluding the entity's liability (see Art. 6(1)(c) of Legislative Decree 231/2001: "persons have committed the offence by fraudulently circumventing the models...").

As pointed out in caselaw, the 'fraud' referred to in Legislative Decree 231/2001 does not necessarily require actual artifice and deception; at the same time, however, fraud cannot consist merely of a breach of the 231 Model's prescriptions. Fraud in this context is held to have occurred if the 231 Model is breached by circumventing the security measures that are in place to ensure its effectiveness.

Based on these principles, for all Sensitive Activities considered to be 'at risk' of 231 Decree offences, the Company's 231 Model has been prepared by including also a Special Part that is reasonably capable of preventing all possible intentional offences, unless an offence has been fraudulently evaded.

3.6 Model Structure

The 231 Model comprises the following main components:

(a) this General Part, which illustrates the 231 Model's overall structure and the set of rules and general principles imposed by it; and

(b) the Special Part, which regulates corporate processes and Sensitive Activities and sets out rules of conduct, prohibitions and control measures to prevent the commission of Offences.

3.7 Criteria for preparing the Model

3.7.1 Phases

In preparing this Model, the Company was inspired by the Confindustria Guidelines.
Consistent with these guidelines, the Model has been prepared by:

- identifying all company processes and Sensitive Activities to verify which areas/sectors of the company are at risk of the Offences being committed; and
- preparing control protocols capable of preventing the identified risks.

The preparation of this Model (and any subsequent updates of a substantial nature) is also supplemented by the following activities:

3.7.1.1 Mapping of risk areas

During this phase, the company's environment is analysed to map all the activities carried out by the Company and to identify which of these activities fall within the scope of being at risk of specific offences being committed (i.e., Sensitive Activities).

The Sensitive Activities are identified via a preliminary examination of the relevant company documentation – which includes Chamber of Commerce company registers, systems of delegated and proxy powers, and company procedures and contracts – and the collection of information from individuals in senior positions and Group Functions.

Together with the identification of potential risks, an analysis is caried out on the control system that the Company uses to prevent the risks of Offences being committed.

3.7.1.2 'Gap analysis'

Based on the results of the above analysis, the Company identifies the actions that need to be implemented within the various Sensitive Activities (*gap analysis*) – at both the level of existing internal procedures and controls and the level of organisational requirements – to define the Model.

3.7.1.3 Changes, updates and continuous improvements of the Model

Subsequent amendments and additions of a substantial nature to the Model itself are to be decided on by the Board of Directors. However, the Chairman of the Board of Directors has the power to make non-substantial amendments or additions to the text. In both cases, the Supervisory Body must be notified of these amendments.

More specifically, the Board of Directors must promptly: (a) amend the Model if significant violations or circumventions of it are identified that show its inadequacy, even if only partial, to guarantee the effective prevention of alleged offences; and (b) update the 231 Model, including at the request of the Supervisory Body, if significant changes occur to the legislative and regulatory system, including internal, governing the Company's activities and/or its structure, organisation or activities.

For the above purposes, the Supervisory Body must provide the board of directors a written report of any circumstances suggesting the need, or even the advisability, to amend or update the 231 Model.

3.7.2 Methodology adopted to prepare the Special Part of the Model

The Special Part of the Model comprises specific control protocols applicable to individual company processes and Sensitive Activities and was prepared in line with the methodology described in § *I. Introduction* of the Special Part, to which reference is made.

3.8 Addressees of the Model

The rules in this Model are addressed to all individuals who are part of the Company's organisation, and in particular:

(a) individuals in positions of representation, administration or management of the Company;

(b) individuals who exercise management and control of the Company itself (even de facto); and

(c) other corporate and/or Group Functions carrying out activities on behalf of and/or in the interest of the Company.

Additionally, the principles of conduct in the Model and several specific rules also apply to Third Parties.

CHAPTER 4: THE SUPERVISORY BODY

4.1 Appointment of the Supervisory Body

Under Art. 6(1)(b) of the Decree, a suitable 231 Model requires a Company to have a body with autonomous powers of initiative and control that is entrusted with supervising the functioning of and compliance with the models and ensuring that they are updated.

To comply with this requirement, the Company has appointed the Supervisory Body.

The Supervisory Body is appointed by a special resolution of the Board of Directors: in this regard, adequate information concerning the professional suitability of its members must be provided at the relevant meeting.

All members of the Company's corporate bodies must be informed of the appointment of the Supervisory Body.

4.2 Eligibility Requirements

The members of the Supervisory Body need to possess adequate requirements of autonomy, independence, professionalism, consistency, honourablility and absence of conflicts of interest.

4.2.1 Strengthened autonomy and independence

The requirement of autonomy and independence presupposes that the Supervisory Body is answerable, in the performance of its function, only to the highest hierarchical level (i.e., the board of directors).

Autonomy and independence must be understood in more than just a formal sense: in other words, the Supervisory Body must be endowed with effective powers of inspection and monitoring and: (a) be able to access relevant corporate information at its own initiative; (b) be provided adequate resources; and (c) be able to make use of instruments, support teams and experts in the performance of its monitoring activities.

More specifically, this requirement is ensured by the board of directors' obligation to approve an adequate annual allocation of financial resources, also at the request of the Supervisory Body itself, which the Supervisory Body can use for any purposes required to properly perform its duties (e.g., specialist consultancy services and necessary travel expenses).

Independence also presupposes that no members of the Supervisory Body find themselves in an actual or potential conflict of interest with the Company or hold executive functions

within the Company that would undermine their objectivity of judgement when verifying compliance with the Model.

Finally, to guarantee the requirements of independence and autonomy, from the appointment date and throughout the duration of the office, each member of the Supervisory Body:

(a) must not serve as a member of the board of directors;

(b) must not be the direct or indirect owner of any Company shares or other shareholdings that are large enough to allow him/her to exercise control or significant influence over the Company;

(c) must not – if external to the Company – directly or indirectly have any economic relations with the Company (or companies controlled by it or connected to it) that are of such importance that they condition their autonomous judgement. This must also be assessed with regard to the subjective financial position of the individual. Each Supervisory Body member also must have no significant business relations with the directors with delegated powers (i.e., executive directors) or shareholders controlling the Company;

(d) must – if internal to the Company – hold a non-executive position and not be directly engaged in business activities, such as individuals engaged in *compliance* and/or *internal audit* functions;

(e) may be a trade union representative;

(f) must not be related to or part of the executive directors' household, where household means the spouse not legally separated and relatives up to the fourth degree of kinship;

(g) must not have any relationship of kinship, marriage or affinity up to the fourth degree with: (i) members of the Board of Directors; (ii) individuals holding representative, administrative or management positions in the Company; (iii) individuals exercising (also de facto) management and control of the Company; or (iv) members of the Board of Statutory Auditors; and

(h) must have and maintain the integrity requirements set out in section 4.2.2.

4.2.2 Honourability and grounds for ineligibility

An individual cannot be appointed to the Supervisory Body if any of the following factors apply, which also result in an individual already appointed to the Supervisory Body being automatically removed from office:

(a) Any of the conditions under Art. 2382 of the Civil Code, i.e., if an individual is incapacitated, disqualified, bankrupt or sentenced to a punishment entailing disqualification (even temporary) from public office or inability to exercise executive offices.

(b) An individual has been subject to preventive measures ordered by the judicial authorities under Law No. 1423 of 27 December 1956 (law on preventive measures against persons dangerous to security and public morality) or Law No. 575 of 31 May 1965 (*anti-mafia* law).

(c) An individual has been convicted by a court decision, including decisions subject to appeal, or subject to a court decision under Arts. 444-*et seq.* of the Criminal Procedure Code, including a conditionally suspended sentence, subject to the effects of rehabilitation:

  (i) for any offences under Title XI of Book V of the Civil Code (Criminal provisions on companies and consortia) or Royal Decree No. 267 of 16 March 1942, as amended or supplemented (Regulations on bankruptcy, arrangements with creditors, receivership and administrative compulsory liquidation);

  (ii) for an offence against public authorities or imprisonment for a term of at least 1 year for an offence against public faith, property, public order or the public economy or a tax offence;

  (iii) to imprisonment for a term of at least two years for any non-negligent offence; or

  (iv) in any event and regardless of the severity of the penalty, for any offences peremptorily provided for under Legislative Decree 231/2001.

(d) An individual has been declared disqualified, incapacitated or subject to bankruptcy proceedings, or has been convicted with a sentence entailing disqualification from: (i) public office; (ii) executive offices of companies and legal persons; (iii) any profession or art; or (iv) the right to contract with the Public Administration.

Similarly, any individual who has been subject to the ancillary administrative penalties under Art. *187-quater* of the Consolidated Law on Finance (Legislative Decree 58/1998) – or who has been sentenced to a penalty entailing disqualification (incl. temporary) from public office

or temporary disqualification from the management offices of legal persons – may not hold the position of Supervisory Body member and, if he/she already does so, automatically ceases to hold office.

4.2.3 Proven professionalism, specific skills in inspection and consultancy work

The Supervisory Body must have technical and professional skills that are appropriate to the functions it performs. These characteristics, together with its independence, guarantee its objectivity of judgement. The Supervisory Body must therefore be chosen from among individuals with adequate professional experience in corporate risk control and management and legal matters.

Additionally, the Supervisory Body may hire external professionals specialised in criminal law, company organisation, auditing, accounting and finance.

4.2.4 Continuity of action

The Supervisory Body must continuously perform all activities necessary for supervising the Model's correct application with adequate commitment and with all necessary investigation powers.

Adequate information on possession of the above requirements must be provided to the Board of Directors when the Supervisory Body is appointed.

4.3 Term of office

Unless the Board of Directors decides otherwise, the Supervisory Body's term of office is set at three years, which may be renewed by a resolution of the Board of Directors.

When the Supervisory Body's term of office expires, it may continue to perform its functions and exercise its powers (as detailed below) until the Board of Directors appoints a new Supervisory Body.

The Supervisory Body may be revoked only for just cause, which must be decided on by a reasoned resolution by the Board of Directors. In this case, the Board of Directors must appoint a new Supervisory Body.

Any of the following constitutes just cause for revocation:

(a) a breach of this Model;

(b) the occurrence of any of the causes of incompatibility referred to in section 4.2;

(c) a conviction of the Company under the Decree, or a plea-bargain sentence that is final, and whose the documentation indicates "omitted or insufficient supervision" by the Supervisory Body under Art. 6(1)(d) of the Decree;

(d) failure to attend more than three consecutive meetings without justification;

(e) negligence in performing their duties;

(f) in the case of individuals who form part of the company structure, any resignation or dismissal or termination of employment; and

(g) a change in the shareholding structure resulting in a change in the person holding the majority of votes exercisable at the Ordinary Shareholders' Meeting.

In the event of resignation or automatic disqualification from the Supervisory Body, the Supervisory Body must promptly notify the Board of Directors, which must take the appropriate decisions without delay.

The Supervisory Body may renounce its appointment at any time by giving written notice with the reasons for the renunciation to the Corporate Bodies. This renunciation takes effect upon acceptance or appointment of a new Supervisory Body and in any case within 60 days from the notification date.

4.4 Function of the Supervisory Body

The Supervisory Body is entrusted with the task of supervision:

(a) of the effectiveness and adequacy of the Model in relation to the corporate structure and its effective capacity to prevent the commission of the Offences;

(b) compliance with the Model by the Addressees; and

(c) of the appropriateness of updating the Model if it needs to be changed because of a change in company and/or regulatory conditions.

On a more operational level, the Supervisory Body has the following tasks:

(a) *Updates, regulatory power, reporting:*

(i) interpret all relevant legislation and verify the adequacy of the Model to meet these regulatory requirements; and report possible areas of intervention to the Board of Directors;

(ii) verify whether the elements required under the Special Part of the Model to prevent specific offences (e.g., adoption of standard clauses and completion of procedures) are in any case adequate and meet all requirements of compliance with the Decree; and, if this is not the case, require that these elements are updated;

(iii) promote the revision and possible updates of the Model in relation to: (1) ascertainment of breaches of the Model; (2) significant changes to the Company's internal structure, business activities or related performance methods; and/or (3) regulatory changes (e.g., new offences added to Legislative Decree 231/2001); and report possible areas of intervention to the Board of Directors;

(iv) promote – if it appears that implementation of the Model is deficient – all necessary initiatives to bring conduct into line with the Model;

(v) coordinate with the heads of the other corporate and/or Group functions for the various aspects relating to the implementation of the Model (e.g., creating standard contractual clauses, training and disciplinary measures);

(vi) periodically verify – with the other competent Functions' support – the system of powers in force; and recommend changes if any management powers and/or qualifications do not correspond with the powers of representation conferred; and

(vii) promptly inform the Board of Directors and the Board of Statutory Auditors of any serious breaches of the Model; and request support from the Functions able to cooperate in verification and identification of suitable actions to prevent the recurrence of the circumstances in question.

(b) *Checks and controls:*

(i) conduct reconnaissance of the company's activities for the purpose of updating the mapping of Sensitive Activities;

(ii) carry out – in accordance with the provisions of the annual schedule of the Supervisory Body's activities – periodic targeted checks on specific operations or acts performed within the scope of Sensitive Activities, the results of which must be summarised in a specific *report* submitted to the competent Corporate Bodies;

(iii) collect, process and store information relevant to compliance with the Model; and update the list of information that must be sent to it or kept at its disposal;

(iv) coordinate with the Functions (also through special meetings) for the best monitoring of Sensitive Activities. To this end, the Supervisory Body has free access to all company documentation (hard copy and computerised) that it considers relevant and must be constantly informed by *management* of: (1) all aspects of company activity that could expose the Company to the risk of any Offences being committed; and (2) relations with Collaborators, Consultants, Partners, Suppliers and Third Parties;

(v) supervise the implementation of the control procedures laid down in the Model;

(vi) promptly verify any criticalities detected by the competent company representatives; and propose appropriate operational solutions; and

(vii) verify whether the corrective actions necessary to make the Model adequate and effective are promptly implemented.

(c) Training:

(i) promote appropriate initiatives for dissemination of knowledge and understanding of the Model; and

(ii) help define training programmes and the content of periodic communications to be made to the Corporate Bodies.

(d) *Violations of the Model and Sanctions:*

(i) if considered necessary to carry out internal investigations, assume a coordinating and supervisory role for these investigations and use – to perform investigative activities – a company and/or Group Function or a combination of Functions and/or external consultants;

(ii) coordinating with the company's *management* to assess or propose the adoption of possible penalties or measures against breaches of the Model. This is without prejudice to the competence of these Functions (particularly HR managers) to issue appropriate decisions and impose penalties (see Chapter 6 of this General Part on this point).

4.5 Powers of the Supervisory Body

The Supervisory Body has, by law, autonomous powers of initiative and control for the purpose of supervising the operation of and compliance with the Model. However, it has no coercive powers or powers to intervene in the corporate structure or impose penalties (these powers are delegated to the competent Corporate Bodies or Functions).

Considering the peculiarities of the attributions and specific professional skills required to perform its supervisory and control tasks, the Supervisory Body must in any case be constantly supported also by the Company's management.

Management, within the scope of their respective functions and within the limits of their assigned powers, is primary responsible for: (a) monitoring activities and areas of competence; and (b) timely and punctual reporting to the Supervisory Body of all anomalies, problems encountered and/or critical issues detected.

The Supervisory Body may request the competent Functions to perform specific monitoring activities to ensure the Model's correct and precise functioning.

All individuals involved within the Company must supervise and inform the Supervisory Body on the correct application of this Model, each within the scope of his or her operational competences.

If it considers it necessary for performance of its supervisory activities and compliance with this Model, the Supervisory Body may request any additional resources from the various Functions with no limits on time or quantity. These resources may also constitute a dedicated full-time or part-time staff if necessary.

Also, if the Supervisory Body requires any professional expertise that the Company does not have, it may hire external consultants.

The Supervisory Body therefore has the power to:

- access all documentation and information relating to the Company;
- use all Functions (who must cooperate) and external consultants;
- collect information from all Addressees of this Model (incl. Third Parties) in relation to all the Company's activities;
- request – through the appropriate channels and individuals – meetings of the Board of Directors and Board of Statutory Auditors to deal with urgent matters;

- request heads of Functions to participate, with no deliberative power, in meetings of the Supervisory Body; and
- use external consultants to delegate circumscribed areas of investigation or activities to. In this regard, the Board of Directors must approve an annual expenditure budget for the Supervisory Body, which has discretion to deploy it for its activities, and supplement this budget for any needs that arise.

4.6 Rules of convocation and operation

The Supervisory Body may regulate how it functions through specific regulations based on the principles set out below:

- The Supervisory Body draws up minutes (at least every six months or upon every relevant event) on the progress of supervisory activities.
- The Corporate Bodies may request that the Supervisory Body be called to meetings of the Board of Directors or the Board of Statutory Auditors at any time.
- Ad hoc meetings may be held with the Functions and all decisions taken during these meetings must be recorded in writing.
- The meeting minutes record all decisions taken by the Supervisory Body and reflect the main considerations made in reaching the decision; these minutes are kept by the Supervisory Body in its archives.

4.7 Reporting by the Supervisory Body

The Supervisory Body reports on the implementation of the Model and the emergence of any critical issues.

Two reporting lines are assigned to the Supervisory Body:

- the first, on an ongoing basis, directly to the Chairman of the Board; and
- the second, on a periodic basis at least once a year, to the entire Board of Directors.

These information flows relate to:

(a) the activities carried out by the Supervisory Body; and
(b) any critical issues (and points for improvement) that have emerged both in terms of internal conduct or events, and in terms of the Model's effectiveness.

In its annual reporting, the Supervisory Body submits to the Board of Directors a written report on the Model's implementation that contains:

(a) a summary analysis of all the activities carried out during the year (indicating in particular the specific controls and checks carried out and their outcome, any updates to the mapping of Sensitive Activities, etc.); and

(b) a plan of planned activities for the following year.

Minutes must be prepared for all meetings with the bodies to which the Supervisory Body reports, and the Supervisory Body must keep copies of these minutes.

The Chairman of the Board of Directors has the power to convene the Supervisory Body at any time, which in turn has the power to convene – through the competent Functions or individuals – meetings of these bodies for urgent reasons.

4.8 Information flows to the Supervisory Body

The Supervisory Body also exercises its verification and control responsibilities through the analysis of systematic information flows.

The above information and documentation to be sent and/or made available to the Supervisory Body, with the relevant timelines and information channels to be used, are identified in the Model's Special Part.

Communication flows to the SB are divided into:

(a) Event-driven flows; and

(b) Periodic flows.

The above information flows must be sent by the competent Functions to the SB's email address: Unikeris.odv@unikeris.com.

Event-driven information flows

Event-driven flows must be sent in written form (to the SB's mailbox: Unikeris.odv@unikeris.com) – or in any other way considered appropriate by the SB – upon the occurrence of specific events that are anomalous or atypical, relate to implementation of the Model and company procedures under the Model, relate to Sensitive Activities or are considered useful for performing the SB's duties.

More specifically, for example, the SB requires written notification of the following events:

(a) any significant enactment, amendment and/or integration of the Company's corporate organisational system and/or corporate structure (extraordinary transactions, etc.), such as amendments and changes to the system of delegated and proxy powers conferred, the organisational chart, etc;

(b) requests for legal assistance forwarded by the Corporate Bodies who are subject to judicial proceedings for offences under the Decree;

(c) inspections performed by public bodies (judicial authorities, Financial Police (*Guardia di Finanza*), other Authorities, etc.) or private third parties (i.e., certification bodies, audits by parties external to the Company);

(d) results of inspections carried out by external Authorities (i.e., the Revenue Agency (*AdE*), Financial Police (*GdF*), Military Police Health & Safety Inspectorate (*Isp. Lav, C.C.*), etc.), from which significant findings, recommendations and/or any sanctions applied to the Company emerge;

(e) measures and/or news indicating that investigative police bodies or any other authority are carrying out investigations or proceedings (incl. against unknown individuals) for offences under Legislative Decree 231/2001 that involve the Company or its representatives, Corporate Bodies, the Functions carrying out activities in favour of the Company, Collaborators, Consultants, Partners or Suppliers;

(f) results of first-level controls, controls carried out to implement the Model and internal investigations from which significant critical issues/anomalies emerge and from which facts, acts, events or omissions regarding criticality/liability for compliance with the Model and its correct implementation emerge;

(g) communications from the Board of Statutory Auditors concerning anomalies/criticalities encountered in assessing and monitoring the adequacy of the Company's organisational structure and internal control system;

(h) significant or atypical financial/corporate transactions that could raise the risk of an offence; and

(i) penalty proceedings carried out and any penalties applied – or orders to dismiss these proceedings with relevant reasons – regarding the commission of Offences or a breach of the Model's rules of conduct or procedures.

In addition to the above event-driven information flows, see the Special Part of the Model for other circumstances that give rise to the obligation to send event-driven communication flows to the SB.

The SB may in any case independently request additional periodical information or news concerning specific situations from any corporate Function or structure. The Functions are responsible for keeping all documentation regarding information sent to the SB available.

Any individual required to submit periodic information flows who breaches the information obligations under this paragraph is subject to a disciplinary penalty. This penalty varies depending on the seriousness of the breach and is set by the Supervisory Body based on the rules under this Model.

Periodic information flows

In addition to the above information to be provided in a timely manner, all Functions and Functions outsourced from other Group companies or Third Parties (as identified in the Special Part) must provide the Supervisory Body all information useful for the purposes of its supervisory activities.

In line with the periodic frequency set out under the Special Part, the designated individual in charge of each respective Function must provide the reported information by email to the SB: Unikeris.odv@unikeris.com.

See the Special Part of the Model for the precise circumstances that give rise to the obligation to send periodic communication flows (e.g., quarterly, half-yearly or yearly) to the SB.

4.9 Reports of conduct relevant to the Model

In addition to the system of information flows outlined above, which is imperative, anyone who becomes aware, by virtue of their duties performed, of unlawful conduct relevant under the Decree or of any violation of this Model must immediately report this through SpeakUp&BeHeard. If any reports prove to be unfounded or made with malice or gross negligence, the measures set out in the Disciplinary System apply.

SpeakUp&BeHeard is the reports management system adopted by the Chiesi Group. This system comprises a web-based platform that does not reside in the Group's IT system and is hosted on an independent server, plus an additional voicemail. It can be accessed by anyone wishing to file a report and provides the possibility for the whistleblower who prefers to report orally to request a direct meeting with the Company.

The system is structured in a way that guarantees (also through computerized methods) the highest levels of confidentiality regarding the reports, the identity of the whistleblower and the individual reported (without prejudice to legal obligations and the protection of the rights of the Company and of individuals wrongly accused and/or in bad faith). It guarantees also the confidentiality, security, non-traceability and integrity of all data relating to the report, in compliance with Decree 24/23. In the case of reports filed using any other methods, the Company is unable to guarantee the same levels of protection. More specifically, if the report is filed by email, anonymity might not be guaranteed.

Reports affecting Unikeris communicated via SpeakUp&BeHeard will be managed by Unikeris Supervisory Body, who holds the requirements provided by Decree 24/23 for the body in charge of managing reports.

In any case, the Company verifies and warrants that whistleblowers will not be subject to any form of retaliation, discrimination or penalization, whether direct or indirect, for reasons connected, directly or indirectly, to the report made. In particular, no one may be subject to any of the retaliatory actions provided for under article 17 of Decree 24/23 (by way of example: coercion, intimidation, discrimination or otherwise unfavorable treatment, early termination or cancellation of the contract for the supply of goods or services), without prejudice to the application of the measures provided for in the Disciplinary System against those who make reports (which turn out to be unfounded) with malice or gross negligence. The process of sending and managing reports and the roles and responsibilities of those involved in the process are set out in the Guideline and SOP titled "Use and Management of SpeakUp&BeHeard".

4.10 Confidentiality obligations

The Supervisory Body must fulfil all tasks with the diligence required by the nature of the task and the activity performed as well as its specific competences.

The Supervisory Body is bound by confidentiality obligations regarding news and information acquired in the performance of its duties.

4.11 Collection and storage of information

Any information collected and any reports received or prepared by the Supervisory Body must be retained for 10 years in a special archive maintained by the Supervisory Body in hard copy or electronic format.

CHAPTER 5: DISSEMINATION AND TRAINING

5.1 Dissemination

In line with the provisions of Legislative Decree 231/2001 and the Confindustria Guidelines, the Company fully publicises this Model through the most appropriate communication channels.

Communication must be widespread, effective, clear and detailed, with periodic updates related to changes in the Model, in compliance with the Confindustria Guidelines.

The adoption of this Model and subsequent updates are sent to: (i) all members of the Corporate Bodies; (ii) the Functions; and (iii) Third Parties.

In the event of resignation and/or revocation of members of the Corporate Bodies or new appointments to the Group Functions, new members must be provided information that ensures that they have all knowledge of primary relevance for the 231 Model.

5.2 Training

Training is restricted to Corporate Bodies and – where the need arises – to Group Functions and/or Third Parties.

This training is managed by the Company under the supervision of the SB and has the objective of ensuring that all individuals involved in performing Sensitive Activities are familiar with the Model adopted by the Company and receive adequate support.

In this respect, a training plan is prepared periodically with the SB's cooperation. This takes into account, in particular, all specific needs that emerge in relation to the specific business operations referred to.

Training must be easy to understand, effective, authoritative, clear and adequately detailed and needs to be repeated at regular intervals.

More specifically, the Company is responsible for adopting and implementing adequate levels of training using appropriate dissemination tools, which includes organising company meetings.

The training content needs to be updated in line with the evolution of legislation and the Model: therefore, in the event of significant changes (e.g., an extension of the Company's administrative liability to new types of offences), the content needs to be consistently supplemented, thereby also ensuring its use.

Non-participation in training activities without justification by members of the Corporate Bodies and/or Group Functions constitutes a breach of all principles contained in this Model and, therefore, are sanctioned in accordance with Chapter 6 below.

The SB periodically checks the status of the training plan's implementation.

CHAPTER 6: THE DISCIPLINARY SYSTEM

6.1 Function of the Disciplinary System

A system of penalties have been created that are commensurate with the related breaches and provide adequate levels of deterrence. These penalties are applied to breaches of the Model's rules and render the SB's supervisory action effective and are intended to ensure the Model's effective implementation.

Under Art. 6(1)(e) of Legislative Decree 231/2001, the creation of this penalty system is in fact an essential requirement of the Model for the purposes of exempting the Company from liability.

The application of penalties and related measures are independent from the direction and outcome of criminal proceedings that judicial authorities bring against conduct that is censured and that also constitutes a relevant offence under Legislative Decree 231/2001. This is because the rules of conduct imposed by the Model are assumed by the Company in full autonomy, regardless of the offence that any conduct amounts to.

Additionally, this Disciplinary System must be adequately disseminated as an integral part of the Model's implementation through adequate information and training activities.

This chapter provides a description of the penalty measures that the Company applies to breaches of the Model by the Addressees.

6.2 Relevant conduct

For the purposes of this Disciplinary System, actions or conduct in breach of the 231 Model adopted by the Company constitute conduct subject to penalties.

The following conduct, among other things, is punishable:

(a) breach of the Model aimed at committing any offences under the Decree or where a danger exists of the Company being held liable under the Decree;

(b) breach of the Model capable of constituting the sole fact (objective element) of any offences under the Decree;

(c) breach of the Model connected in any way to 'crime risk' areas or Sensitive Activities;

(d) breach of internal procedures referred to in this Model;

(e) failure to cooperate with the Supervisory Body when requested;

(f) repeated failures to send information flows/reports required under the Model that are intended to obstruct the Supervisory Body's functions; and

(g) repeated non-participation in training on the Model with no adequate justification.

Additionally, disciplinary penalties can be applied against:

(a) whoever files reports (which turned out to be unfounded) with malice or gross negligence;

(b) whoever (i) adopts retaliatory actions, according to article 17 of Decree 24/23, against the whistleblower (and/or the further persons/entities reported under article 3.5 of Decree 24/23), for reasons connected, directly or indirectly, to the report made; (ii) breaches the confidentiality protection measures set out by article 12 of Decree 24/23 for the whistleblower, the persons involved and persons mentioned in the reported conduct; (iii) hampered or attempted to hamper report submission;

(c) the persons involved who turn out to be responsible for the reported conduct.

The system of penalties is subject to constant verification and evaluation by the Supervisory Body and the Board of Directors, which is responsible for the concrete application of the disciplinary measures outlined below at the possible proposal of the Supervisory Body.

If the conduct in question constitutes a relevant offence under Legislative Decree 231/2001, the activation of the Disciplinary System takes place irrespective of the conduct and outcome of any related criminal proceedings.

6.3 Penalties

The identification and imposition of penalties must consider the principles of proportionality and appropriateness regarding alleged breaches.

In this respect, the gravity of each breach is assessed based on the following circumstances:

- the concrete timing and methods of the breach;
- the presence and intensity of intent;
- the level of responsibility and autonomy of the individual who committed the breach;
- the extent of the harm or danger arising from the breach to the Company; and
- the circumstances under which the breach took place.

Recidivism constitutes an aggravating circumstance and implies the application of a more serious penalty.

The application of the penalties set out below are in any event without prejudice to the Company's right to take action against the liable party to obtain compensation for damage suffered as a result of or as a consequence of the conduct ascertained.

6.4 Measures against directors and attorneys

If a director or an attorney is discovered to have breached the Model, the Supervisory Body must file a report with the Board of Directors and the Board of Statutory Auditors that contains the details of the conduct, the documentary evidence and a possible proposal for an appropriate penalty.

The Board of Directors may carry out further investigations and, based on the results, assess which penalty to apply, giving reasons for any disagreement with the proposal submitted by the Supervisory Body.

More specifically, the following penalties apply:

- a written warning;
- an order to immediately comply with the Model; or
- removal from office.

6.5 Measures against auditors

If the SB discovers that a member of the Board of Statutory Auditors has breached the Model, it must file a report with the Board of Directors and the Board of Statutory Auditors that contains details of the conduct, the documentary evidence, and a possible proposal for an appropriate penalty.

The Board of Directors may carry out further investigations and, based on the results, assess which penalty to apply, giving reasons for any disagreement with the SB's proposal.

More specifically, the following penalties may be applied:

- an order to immediately comply with the Model; or
- revocation of the assignment.

6.6 Measures against Third Parties

If the Supervisory Body discovers that the Model has been breached by any Third Parties, it must file a report with the Department in charge of managing the contractual relationship in question that contains details of the conduct, the documentary evidence and a possible proposal regarding the appropriate penalty.

The department concerned decides on the determination and concrete application of the measure, justifying any disagreement with the proposal formulated by the SB.

The Function then sends to the Third Parties a written notification that indicates the challenged conduct, the provisions of the Model that have been breached and the contractually applicable remedy. The Function concerned must also ensure the effective application of the penalty in compliance with all applicable laws and regulations.

The SB – which is provided the above information – verifies the application of the applicable contractual remedy.

CHAPTER 7: CHECKS ON THE MODEL'S ADEQUACY

The actual application of the Model and its effective implementation are subject to appropriate control activities.

These activities are carried out primarily by the competent Functions.

The Supervisory Body conducts ongoing supervision of the Model's effectiveness, which takes the form of verifying whether the concrete conduct of the Recipients complies with the Model itself. In addition to this, the Supervisory Body also periodically carries out specific checks on the Model's suitability for preventing Offences from being committed and on its compliance with the legislation on the administrative liability of entities. This forms a part of the periodic updates to the Model.

Finally, the Supervisory Body reviews all reports received during the year, all events considered risky, all actions taken by the Supervisory Body and the Corporate Bodies' awareness of issues regarding corporate criminal liability through spot checks.

In carrying out its checks, the Supervisory Body normally obtains support from the heads of each competent Function and, where necessary, external consultants.

The audits and their outcomes are subject to an annual report filed with the Board of Directors. More specifically, in the event of a negative outcome, the Supervisory Body must set out all improvements to be implemented in the plan for the year.

CHAPTER 8: THE COMPONENTS OF THE MODEL

8.1 The Elements of the Model

This 231 Model is structured across the following three levels: (1) organisation; (2) general control mechanisms; and (3) specific control protocols.

8.2 Organisational Elements of the Model

The organisational components of the Company's 231 Model comprise:

- **Internal rules**: the rules under this Model, including the rules of conduct, prohibitions and control provisions in the Special Part of the Model; as well as the specific rules of conduct, policies and procedures adopted by the Company to implement the Model.

- **Organisational structure:** the presence of a corporate organisation that: (a) is consistent with the company's activities and suitable for ensuring correct conduct; and (b) guarantees a clear and organic allocation of tasks and an appropriate segregation of functions, ensuring that the arrangements envisaged by the organisational structure are actually implemented and subject to control through: (i) service contracts with Group companies or third parties, to which specific corporate activities are outsourced; and (ii) a formalised framework of powers (proxies and powers of attorney), which constitutes an integral and substantial part of the Model.

- **Supervisory Body**: this is the body that is created by virtue of the Model and endowed with autonomy, independence, continuity of action and professionalism. It has the task of supervising the operation of and compliance with the Model and proposing its updates. It is endowed also with the capacity to fund and support the Functions and the power to access company information.

8.3 The general controls

The general safeguards below are envisaged as an essential part of the Model that must always be applied and complied with regarding all Sensitive Activities detailed under the Special Part of the 231 Model.

8.3.1 The Code of Conduct

The adoption of ethical principles relevant to the prevention of offences under Legislative Decree 231/2001 is an objective of this Model.

In this perspective, the adoption of a Code of Conduct as a useful governance tool constitutes an essential element of the preventive control system. The Code of Conduct, in fact, aims to recommend, promote or prohibit specific conduct that is subject to penalties in proportion to the seriousness of the breaches committed.

The rules of conduct under this Model are integrated with those of the Code of Conduct, although the Model has a different scope from the Code of Conduct in terms of the purposes it intends to pursue in implementing the provisions of the Decree.

The Code of Conduct expresses the principles of "company deontology", which Chiesi recognises as its own and requires the whole Group to comply with. This fulfils a twofold function: on the one hand, it defines the values and ethical principles that inspire the Group in the performance of its corporate mission; on the other hand, it identifies specific behavioural norms that all the recipients of the Code of Conduct must follow.

8.3.2 The Anti-Bribery Policy

On 5 December 2022, the UNIKERIS Board of Directors approved the Chiesi Anti-Bribery Policy. The Policy is a Group document that sets out a set of common anti-bribery rules applicable to all internal and external stakeholders of the Group.

8.3.3 System of powers

The Company adopts a system of powers that it keeps up-to-date over time and that is based on delegations of authority, powers of attorney and approval protocols for internal costs and bank account transactions.

These powers are strictly connected and consistent with the organisational and management responsibilities assigned and circumscribed to specific value limits.

The allocation of powers is in accordance with the following mandatory principles:

- definition of roles, responsibilities and controls in the conferral process;
- the granting, updating and revocation of powers consistent with the roles held in the organisation, with alignment in the event of changes to the organisation or individual roles and responsibilities or exits/entries of individuals;
- timely and continual dissemination of information regarding ownership of the powers granted and changes to them;
- traceability and archiving of all documentation relating to powers granted and variations of them;

- periodic verification of conformity of the exercise of powers of representation with granted powers of attorney; and
- periodic monitoring of the adequacy of the system of powers and all updates, with particular regard to any developments in the Company's business.

8.3.4 Segregation

The performance of Sensitive Activities must be based on the principle of segregation of duties: an individual who takes the decision and implements it must be as different as possible from the person in charge of carrying out the controls. The segregation of duties must be ensured by the intervention of several individuals within the same process and may be implemented through the use of computer systems that allow only specific identified and authorised individuals to perform specific operations. If segregation of duties cannot be fully ensured, compensatory controls are provided for.

The purpose of this safeguard is to prevent a person from being able to conceal errors or irregularities regarding a transaction committed in the performance of his or her duties without other colleagues engaged in the same transaction noticing the error or irregularity. The fundamental consequence of this is that an irregularity could only occur in the event of collusion between two or more managers.

8.3.5 Traceability and archiving

All Sensitive Activities must be organised in a way that ensures the documentary traceability and *ex post* verifiability of each relevant step of the process; as well as the correct and documented filing and storage of the relevant documentation related to each process through computerised and/or paper methods.

The purpose of this control is to ensure that all corporate transactions are authorised at a predefined level and that they are supported by adequate documentation that ensures transparency of the transactions themselves and facilitates their verification at any time.

8.3.6 Management system for outsourced processes

Processes outsourced to other Group companies or Third Parties are punctually identified in the Special Part of the Model.

Recourse to the outsourcing of functions entails significant benefits for the Company which, given its small size, could not otherwise equip itself with an internal structure capable of adequately managing all processes. At the same time, however, the Model requires outsourced activities to be adequately regulated by contracts that envisage, depending on each case:

- the manner in which the outsourced activities are to be carried out and the related remuneration and adequately define these points;

- that the supplier must perform the outsourced activities in compliance with current and applicable external and Company regulations;

- that the supplier has all necessary authorisations to carry out the assignment;

- that the supplier guarantees – as far as possible – the continuity of the service and security and confidentiality of all data relating to the Company;

- that all Functions of the Company have – as far as possible – access to and control over the supplier's activities and documentation;

- that the Company has adequate remedies for a breach of contract; and

- that the supplier must ensure that all activities are carried out in compliance with applicable laws and Group policies (as stipulated in section 8.3.8).

8.3.7 Cash flow management and control system

Financial management is supported by structured expenditure authorisation processes and dedicated IT tools set up on workflows consistent with formally defined spending powers and organisational roles.

These systems and processes are inspired by the principles of:

- separation of duties (the individual requesting the expenditure must not also be the individual authorising it, who must not also be the individual who materially makes the payment and records it);

- traceability of all financial movements and reconciliation of them with the administrative accounting system;

- identification of the reasons for the expenditure to be incurred; and

- provision of standard forms of payment.

8.3.8 Checks and monitoring

The Model requires the performance of verification activities (periodic or ad hoc) related to each Sensitive Activity and the monitoring of Sensitive Activities in accordance with the Model's provisions.

8.3.9 Information flows

The Model requires that the individual in charge of the Sensitive Activity/Process considered from time to time notifies the Body of any relevant information related to the specific activity/process, particularly any knowledge of situations in which the Sensitive Activity/Process was performed in breach of company guidelines or procedures in force. This also requires the preparation and updates of periodic summary reports with relevant information related to the Sensitive Activity/Process considered from time to time.

8.3.10 Contractual clauses

Contracts regulating the performance of Sensitive Activities must include special clauses aimed at protecting the Company from conduct by its contractual counterparts that breaches the Model and the company procedures that implement it. These clauses should include, for example, where applicable: (a) a declaration by the counterparty that it is aware of and undertakes to comply with the Anti-Bribery Policy and Code of Interdependence for Suppliers adopted by the Group; (b) the Company's right to terminate the contracts in question for a breach of these obligations; and (c) a reference to any other relevant clauses under the Model, where relevant.

8.4 Control Protocols of the Special Part

In addition to the general controls described above and those already adopted by the Company, specific control protocols defining rules of conduct, prohibitions and control measures associated with the Company's Sensitive Activities must be adopted.

The Control Protocols form the Special Part of the 231 Model.

Organisation, management and control model under

Legislative Decree 231/2001

SPECIAL PART

NO. VERSION	DATE	NOTES
01	**31 May 2023**	First issue
02	**12 April 2024**	Second issue
03	**June 2026**	Third issue

Index

1 FOREWORD 4

2 GENERAL PRINCIPLES OF CONDUCT 7

3 SENSITIVE 231 PROCESSES 9

3.1 Regulatory and Pharmacovigilance 9

3.2 Management of Product Marketing/Supplying Activities 13

3.3 Management of legal and corporate affairs 19

3.4 Intellectual Property 25

3.5 Information Technology 29

3.6 Finance and Taxation 33

3.7 Non-core purchases 39

4 INFORMATION FLOWS 45

Attachments:

A. Risk Assessment – Mapping Processes – Functions – Offences – Controls

1. FOREWORD

Before the adoption of the current Model, UNIKERIS carried out a *risk assessment* to identify the Sensitive Activities, i.e., activities exposed to the risk of the commission of Offences under Legislative Decree 231/2001. After identifying the Sensitive Activities related to each corporate process, the respective Control Protocols reflected in this Special Part were then prepared, i.e., the rules of conduct, prohibitions and controls aimed at preventing, for each corporate process, the commission of the Offences.

For the purposes of carrying out this *risk assessment*, *workshop* sessions were organised with individuals responsible for carrying out the Company's activities, during which the purpose of the *risk assessment* was illustrated and the characteristics and methods of carrying out each Sensitive Activity in relation to the relevant crime risk scenarios were briefly reviewed. This permitted the identification of control measures already implemented and adopted by the Company in the context of carrying out the Sensitive Activities and an assessment of the 231 risks inherent in each activity.

The Annex titled "*Risk Assessment – Mapping Processes – Functions – Offences – Controls*" contains the following for each Process:

- Predicate Offences that the Company is potentially exposed to in relation to each Process; in this regard, the exposure to risk can be "direct", in cases where the corporate activity is improperly conducted to commit the Offence, or "indirect" or "instrumental" if the activity is improperly conducted to facilitate or conceal the commission of an Offence in the context of another corporate activity.
- Possible ways of carrying out risk offences.
- Parties involved in each Sensitive Activity, with particular regard to the Company and/or Group Functions, as well as Third Parties, Collaborators, Consultants, Partners, Suppliers and any P.A.'s/Public Officials involved.
- Horizontal controls, i.e., the general controls that are envisaged as an essential part of the Model and that must always be applied and respected in relation to all Sensitive Activities taken into consideration by this Special Part of the 231 Model (e.g., segregation of duties, traceability and archiving and power system).
- Vertical controls, i.e., the specific control measures, including procedural measures, adopted by the Company in relation to each Sensitive Activity.

At the outcome of the *risk assessment* activities, the risk of Offences being committed is considered, on the whole, to be limited. The design of this Special Part was therefore based on a criterion of proportionality, whereby the rules and controls established are proportionate to the Company's small size and structure.

This Special Part indicates the Processes that characterise the Company's operations, the related Sensitive Activities – carried out by the Company both directly and through other Group companies and/or Third Parties – and the respective Control Protocols. The following are indicated for each Process:

a. **Sensitive Activities**: description of the Sensitive Activities relating to each Process;
b. **Predicate Offences**: the Offences relating to each Sensitive Activity;
c. **Rules of Conduct**: the rules of conduct to be observed by the main parties involved in the Process;
d. **Prohibitions**: the prohibitions to be observed by the main parties involved in the Process;
e. **Specific Controls**: the controls to be implemented by the relevant corporate functions in the performance of their activities; and
f. **Procedural Controls**: the company procedures governing the Sensitive Activities covered by this Special Part.

More specifically, specific 'process hubs' have been identified and enhanced that provide for controls that cannot be circumvented even in the event of a 'frontal violation' of the rules. This is to ensure that the application, monitoring and auditing of the Model is more effective ("**Control Points**").

The methodology described above will also be adopted upon each subsequent update of the Model or if the interventions are of a substantial nature and therefore entail the identification of new Sensitive Activities, the assessment of new Offences or the introduction of new Control Points.

This Special Part constitutes an integral part of the UNIKERIS Model and applies – to the extent of their respective relevance – to all Recipients of the Model who are involved in the performance of Sensitive Activities, including:

- individuals in positions of representation, administration or management of the Company; and

- Partners, Suppliers, Collaborators, Consultants and, in general, Third Parties operating in the name of or on behalf of or in the interest of the Company, under the supervision of senior persons.

Any breach of this Special Part entails the application of disciplinary penalties, in accordance with the law, current contractual regulations and the disciplinary system adopted by the Company (see General Part of the 231 Model).

All terms indicated with a capital letter in this Special Part have the same meaning as the meaning given to them in the General Part of the Company's 231 Model.

For the purposes of this Special Part, the following definitions are also relevant in addition to those indicated in the General Part:

1. "Recipients": the subjects identified in the paragraph titled "Recipients of the Model" in the General Part.
2. "Company procedures": policies, guidelines, operating instructions, company and/or Group SOPs relevant to the performance of Sensitive Activities;
3. "Processes": macro areas of activity into which the Company's operations are organised; and
4. "Control Protocols": the rules of conduct, prohibitions and controls aimed at preventing with regard to each Process, the Commission of Offences.

2. GENERAL PRINCIPLES OF CONDUCT

The Addressees of the Model, as well as Third Parties involved in any capacity in Sensitive Activities, must:

- comply with the relevant legal provisions, as well as the general principles referred to in the Group Code of Conduct and the applicable company procedures;
- comply with the tasks, roles and responsibilities set out by the system of powers, as well as all service contracts entered into by the Company in connection with the performance of Sensitive Activities;
- refrain from conduct that would amount to the relevant Offences for Sensitive Activities;
- refrain from engaging in conduct that, even if it does not constitute offences per se, could constitute activities instrumental to the commission of these offences. 'Instrumental' in this sense means those activities that, combined with directly sensitive

activities, support the commission of the offence and thus constitute its implementation method; and

- promptly notify the company management or its company contact person (if external) of any exceptions to the control measures laid down in this Model or in company procedures.

Third Parties are also required to promptly inform their company contact person if they become aware of any fact that could materially affect their ability to perform the outsourced activities in accordance with the contract.

In fact, because UNIKERIS does not currently have any employment relationships, the Company has outsourced corporate activities under specific contracts to: (a) third parties (incl. Third Parties); and (b) other Group companies (with the support of specific corporate functions).

With regard to the outsourcing of business activities under point (a) above, the Third Parties provide the Company services relating to, among other things, the distribution of the Product, management and execution of orders for the Product, and participation in procedures called by the Public Administration for the supply of the Product.

On the other hand, with regard to the outsourcing of business activities under point (ii), the Chiesi Group companies that are primarily involved are: (a) Chiesi Limited, which, through functions/employees based in the UK, provides the Company a range of services (e.g., customer service, medical liaison services, medical affairs, management, financial services, consultancy and assistance for all matters relating to human resources management, legal services, company secretarial services, support services and regulatory and quality assurance services); and (b) Chiesi Farmaceutici S.p.A., which, through functions/employees based in Italy, provides managerial support services, management of tax compliance relating to the secondary office and intellectual property.

In addition to the information already outlined in the General Part (8.3.4.), service contracts need to regulate the way that outsourced activities are performed and commit the Third Parties to the proper performance of the activity in compliance with applicable regulations and corporate provisions (e.g., the Code of Conduct, Supplier Interdependence Code and Anti-Bribery Policy adopted by the Group).

In the performance and delivery of outsourced services and where practicable, the company must:

- check that assignments given to Third Parties are in writing and contain (where practicable) a clause stipulating compliance with the company's provisions;
- ensure that contracts with Third Parties - depending on the nature, complexity and/or value of the assignment - envisage the possibility for the Company to carry out checks – also on a sample basis – on the activity performed by the counterparty under the contract;
- ensure that relations with Third Parties involved in the management of Sensitive Activities take place in full compliance with applicable laws and regulations; - monitor and periodically evaluate the performance of Third Parties.

3. SENSITIVE 231 PROCESSES

3.1 REGULATORY AND PHARMACOVIGILANCE

Sensitive Activities

This Process includes the following Sensitive Activities in particular:

- ❖ Management of relations with competent authorities;
- ❖ Handling of complaints and reports on Product quality; and
- ❖ Managing the reporting of adverse drug reactions.

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 24 - Misappropriation of funds, fraud to the detriment of the State, a public body or the European Union or for the purpose of obtaining public funds, computer fraud to the detriment of the State or a public body and fraud in public procurement;
- Art. 25 - Embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office; and - Art. 25 ter - Corporate offences.

Rules of Conduct

When performing the Sensitive Activities referred to in this Process, all Addressees must observe the rules of conduct set out below:

Management of relations with competent authorities, *Management of product quality complaints and reports* and *Managing the reporting of adverse drug reactions*

- Manage relations with the Authorities exclusively through individuals with appropriate powers and in full compliance with the law, current regulations and the principles of transparency and fairness.
- In the event of audits and inspections by external public authorities/bodies:
  - ensure the participation in these audits/inspections of at least two different and endowed with appropriate powers;
  - ensure the traceability of all audits or inspections through the preparation of an appropriate report or minutes;
  - email their contact persons on the outcome of the audit/inspection; and
  - in the event of findings by external Public Authorities/Bodies, prepare a specific improvement plan that identifies nonconformity and/or irregularities observed by the inspectors during the visit and defines any corrective actions, the functions responsible and the timeframe for their implementation.
- In the management of communications with authorities:
  - operate with fairness and impartiality through the corporate communication channels designated for that purpose;
  - represent the interests and positions of the Company in a truthful, transparent and consistent manner, avoiding any exposure of untrue, incomplete or misleading information or statements to procure an undue advantage to the Company; and
  - if documentation to be submitted is produced with full or partial support of Third Parties or other Addressees of the Model, ensure that the selection of these parties is always carried out in compliance with the requirements of professionalism, independence and competence.
- In the event of non-compliant requests by an authority representative:
  - do not comply with the request; and
  - provide timely information to the company's management.
- Comply with all measures set out by the competent authorities in the event of complaints or reports concerning the Product's quality.

Managing the reporting of adverse drug reactions

- Ensure that those involved are adequately informed about how to file a report and how to report adverse drug reactions.
- Ensure that report are filed with the Authorities:

- in a timely manner and in accordance with the principles of diligence and professionalism so as to provide clear, accurate, complete, truthful and true information;
- together with the relevant forms and documentation;
- by accessing the relevant Agency's database using personal user IDs and passwords and by the individuals previously identified and authorised or by individuals specifically delegated by them.

Prohibitions

In any case, it is forbidden to engage in/collaborate in/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. For example, it is forbidden to:

- submit untrue statements or documentation to authorities or their representatives to obtain undue advantages (e.g., to obtain a marketing authorisation or reimbursement of a drug);
- giving or promising money or other benefits to intermediaries as consideration for unlawful mediation whereby these intermediaries exploit existing or alleged relations with public entities to influence Authorities' decisions/actions for the Company's benefit;
- establish collaborative relations (remunerated in any way) with employees, collaborators or interns of Authorities and adopt conduct aimed at unduly influencing their judgement/opinion;
- engage in conduct contrary to the ethical principles adopted by the Company that is aimed at expediting the procedural process of dossiers, setting legal deadlines or obtaining information that falls within the definition of "confidentiality" under Art. 3 of Ministerial Decree 353/1997 or that is in any case excluded from the right of access by specific regulations;
- promising or paying money (incl. through third parties) to representatives of authorities or private individuals (e.g., patients, pharmacies and distributors), also in a personal capacity or as a result of unlawful pressure, to specifically prevent – respectively – a complaint from being followed up on or a report from being filed;
- promising or paying money (incl. through third parties) to representatives of Authorities, also in a personal capacity or as a result of unlawful pressure, to influence the assessment of defects subject to a complaint/report so as to ensure that their seriousness and danger is underestimated;

- Promising or paying money (incl. through third parties) to representatives of Authorities, incl. in a personal capacity or as a result of unlawful pressure, to prevent – following a complaint/report – the dissemination of communications relating to Product defects both through portals operated by the Authorities and the media and the adoption of measures against the Company; and
- conceal or destroy correspondence or any other documentation produced that relates to the Sensitive Activities described in this Process.

Specific checks

With specific regard to the *Management of complaints and reports on Product quality* and the *Management of reports of any adverse drug reactions*, the following checks are performed (by the Head of Quality Function of Chiesi Ltd, Pharmacovigilance Function of Chiesi US, and Customer Service Function of Chiesi Farmaceutici S.p.A., to the extent of their respective responsibilities):

- ✓ verification of the completeness, accuracy and correctness of any reports received from the customers; and
- ✓ ensure that all reports received from the customer are promptly forwarded to the manufacturing sites for subsequent the investigation activities.

Procedural controls

The following company procedures that are adopted by the Company and/or the Group and that regulate and govern the Sensitive Activities covered by this Process are considered applicable:

o Quality Policy. o Quality Manual; o Site Master File; o UKUNK-SOP-QA-0001, Supply of the Product as an unlicensed medicine.

The above rules, prohibitions and specific controls applicable to the Sensitive Activity *Management of relations with competent authorities* extend – even where not expressly provided for – to all the other Sensitive Activities in which Public Administrations and/or Public Officials are involved.

3.2 MANAGEMENT OF PRODUCT MARKETING/SUPPLYING ACTIVITIES

Sensitive Activities

This Process includes the following Sensitive Activities in particular:

- ❖ Handling of product supply requests and unsolicited requests by HCPs;
- ❖ Customer qualification;
- ❖ Participation in public and private tenders and direct negotiations;
- ❖ Product supply/logistics management; and
- ❖ Management of importation activities and related VAT customs requirements.

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 24 – Misappropriation of funds; fraud to the detriment of the State, a public body or the European Union or for the purpose of obtaining public funds; computer fraud to the detriment of the State or a public body; and fraud in public procurement;
- Art. 25 - Embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office;
- Art. 25*ter* - Corporate offences;
- Art. 25 *octies* - Receiving stolen goods; money laundering; use of money, goods or benefits of unlawful origin; and self-laundering; and
- Art. 25*quinquiesdecies* - Tax offences.

Rules of conduct

When performing the Sensitive Activities referred to in this Process, all Addressees are required to observe the rules of conduct set out below:

Handling of product supply requests and unsolicited requests by HCPs

- Ensure maximum transparency and avoid any anti-competitive conduct.
- Avoid conduct likely to infringe the industrial and/or intellectual property rights of others.

Customer qualification

- Comply with national and supranational regulations on customer qualification.
- Conduct themselves in a way that ensures free and proper conduct of trade and lawful competition in compliance with public faith.
- Behave in a way that does not compromise the other party's good faith.
- Ensure that the Product supplied by the Company can be sold to the requesting customers/patients.

- Formalise the criteria based on which a client/patient can be 'deleted' from the company's internal lists.

Participation in public and private tenders and direct negotiations

- Clearly identify the roles and responsibilities of the Functions involved in Sensitive Activity, with particular regard to: (a) the fulfillment of all obligations imposed by the laws in force; (b) the identification of all individuals in charge of preparing documentation to be sent to public bodies; (c) the prior authorisation by the Company regarding participation in public and private tenders by third parties
- Constantly monitor private tenders/tenders and direct negotiations with the PA with special referenceand to the evolving stages of tender procedures and of negotiations
- Monitor third parties' (i.e. Interlabo) compliance with the contractual terms agreed with the Company regarding the procedures for its participation in private tenders/tenders and direct negotiations with the PA.

Product supply/logistics management

- Ensure that all Logistics Suppliers involved in the management of Sensitive Activity store the Product in accordance with specific storage conditions and ensure its proper maintenance before marketing/supplying it.
- Maintain relations exclusively with suppliers who guarantee high standards in the adoption of appropriate accident prevention measures to protect their workers and who guarantee that their workers work under healthy, safe and decent working conditions.

Management of importation activities and related VAT customs formalities.

- Ensure compliance with all applicable legal regulations regarding importation activities of the Product, incl. tax and customs matters.

- Avail itself of the support of freight forwarders, customs agents and/or external agencies experienced in customs matters and with whom specific mandates are entered into.
- Guarantee that the Product (and/or its packaging and/or labelling) cannot be altered, modified, manipulated and/or tampered with in any way that compromises its quality.
- Ensure the identification of all competent Functions involved in activities relating to the management phases of relations with customs (preparation of all necessary documentation, verification of its completeness and accuracy, and its approval).

- Ensure that all individuals handling customs formalities on behalf of the Company have the necessary authorisations/certifications (e.g., registration in the single national register for customs officers and A.E.O. certificate for international forwarding agents).
- Ensure that, in the performance of activities by forwarders/customs agents/agencies, the following are ensured: (a) transparency and traceability of activities performed; and (b) internal reporting. In particular, all importation operations performed must be tracked.
- Prepare and submit customs declarations, also through third parties, providing truthful data and information (e.g., tariff code, origin, value and quantity) and correctly pay VAT.
- Define how any irregularities are to be reported to the competent authorities in accordance with all applicable regulatory provisions related to the individual incident.
- Require third parties supporting the Company to promptly inform the Company contact person of any fact that could materially affect their ability to perform the outsourced activities in compliance with the regulations in force. More specifically, forwarding agents/customs agents/agencies must inform the Company of any anomalies encountered in the management of dossiers.
- Manage relations with customs authorities (i.e., with other competent public authorities) exclusively through individuals with appropriate powers and in full compliance with the law, current regulations, and the principles of transparency and fairness.
- In the event of audits and inspections by customs authorities:
  - ensure the traceability of all audits or inspections through the preparation of an appropriate internal report or minutes;
  - email their contact persons on the outcome of the audit/inspection; and
  - in the event of findings by the authorities, prepare a specific improvement plan that identifies the non-conformities and/or irregularities observed by the inspectors during the visit and sets possible corrective action.
- In managing communications with the authorities:
  - operate with fairness and impartiality through the corporate communication channels designated for that purpose;
  - represent the interests and positions of the Company in a truthful, transparent and consistent manner, avoiding any exposure of untrue, incomplete or misleading information or statements to procure an undue advantage to the Company; and
  - if the documentation to be submitted is produced with full or partial support of third parties (consultants, technical experts, etc.), ensure that the selection of these

parties is always carried out in compliance with the requirements of professionalism, independence and competence.

- Ensure that all Suppliers involved in the management of Sensitive Activities (incl. freight forwarders/customs agents/agencies) are subject to an evaluation process consisting of: (a) a compliance audit; and (b) an HSE audit.

Prohibitions

In any case, it is forbidden to engage/collaborate/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. More specifically, for example, it is forbidden to:

- submit untruthful declarations or documents to public authorities or their representatives to obtain undue advantages;
- give or promise money or other benefits to intermediaries as consideration for unlawful mediation whereby they exploit existing or alleged relations with public entities and exert influence on the Public Administration to influence its action to the benefit of the Company;
- establish collaborative relations remunerated in any way with employees, collaborators or interns of Public Administrations and engage in conduct aimed at unduly influencing their judgement/opinion;
- enter into competition-restricting agreements with third-party partners and/or customers and/or distributors, incl. through agents;
- sell products at particularly advantageous prices to obtain undue advantages over competitors;
- market/supply products that do not have the relevant authorisations, incl. customs authorisations, and/or that have not undergone the specific quality controls provided for by the applicable regulations and the company's own regulations;
- supply products of a quality other than that stated or agreed;
- engage in conduct likely to infringe the industrial and intellectual property rights of others;
- carry out promotional and marketing activities on the Product;
- conceal or destroy correspondence or any other documentation produced that relates to the Sensitive Activities referred to in this Process.

Participation in public and private tenders and direct negotiations

- Promising or paying money, goods in kind or other undue benefits to public or private entities in order for them to accept the Company's bid in a tender or of a direct negotiation.
- Sharing false information on the Company and/or the products it markets/supplies with a Public Administration or entering this false information into a Public Administration's software.
- Unauthorised access or damage to the contracting authority's software.
- Modifying documentation regarding product characteristics to make it comply with the requirements of a tender.
- Agreeing with a partner or client to obtain undue benefits from participation in a tender.
- Illegally intercede with a public official or a private counterparty to have the client or partner awarded the tender.
- prevent or disturb a tender in public enchantments or private licitations on behalf of public administrations, or remove bidders, by violence or threat, or by gifts, promises, collusion or other fraudulent means.
- disturb the administrative procedure aimed at establishing the content of the notice or other equivalent act through violence or threat, or through gifts, promises, collusion or other fraudulent means, in order to influence the methods of choosing the contractor by the public administration.

Management of importation activities and related VAT customs formalities.

- Omitting or delaying the lodging of a customs declaration or improperly handling customs formalities by providing false information on the quantity, quality or value of goods.
- Fraudulently evading payments of customs debts.
- Preventing goods from being subject to the customs control system of assessing and collecting border duties, either by failing to declare them to the customs authorities or by concealing them or falsifying the transport and/or commercial documentation (e.g., by stating on the customs documents that the goods have a reduced value compared to the value normally indicated for similar goods coming from the same country of origin; or if the documents certifying transport indicate a quantity of goods that is less than the excess quantity ascertained during the visit by the delegate for control).

- Improperly using foreign goods imported/exported free of duty and with a reduced border duty, by allocating them or using them in a way that is different from the purpose for which the relief or reduction was granted.
- Bringing foreign goods into the State as substitutes for national or nationalised goods sent into circulation.
- Evading the payment of border duties through the artificial manipulation of the goods or fraudulent means.

Specific checks

With specific reference to the Handling of product supply requests and unsolicited requests by HCPs and *Customer Qualification*, the head of Quality Function of Chiesi Ltd carries out the following checks:

✓ Checks aimed at initial qualification and maintenance of qualification over time for each client/patient.

With specific regard to *Participation in public and private tenders and direct negotiations*, the following checks are carried out:

✓ Granting of prior and express authorization in favor of third parties (i.e. Interlabo) for participation in public and private tenders in the name and on behalf of Unikeris;

✓ Checking documentation to be submitted for tender/private treaty/*direct negotiations* /tender (check list and required documentation) to verify the completeness and accuracy of the documentation.

✓ Verification that information provided to the Public Administration corresponds to the information in public tenders (also in terms of modalities, timing, quantity and quality).

✓ Verification of all tenders that the Company has participated in and/or intends to participate in by analysing the periodic reports prepared by the Special Prosecutor.

With specific regard to the Management of *product supply/logistics* and to the *Management of importation activities and related VAT customs formalities*, the following checks are carried out (by the head of the competent Tax Function):

✓ Regulatory monitoring, also with the help of external consultants, to detect new regulatory and/or caselaw and/or new best practices relevant to imports/exports.

✓ Audits aimed at the initial qualification and maintenance of qualification over time of each Supplier/Third Party, possibly also by carrying out on-site audits.

- ✓ Checks on the appropriateness of all sums paid to forwarding agents/customs agents/agencies (i.e., fees for services rendered, reimbursements of expenses and customs charges).
- ✓ Checks on customs operations carried out by external parties in the name and on behalf of the Company. More specifically, the Company monitors all activities of forwarding agents/customs agents/agencies in relation to the effectiveness of the service provided.
- ✓ Verification of customs declarations and the correctness and accuracy of the data entered in them.

Procedural controls

The following company procedures, adopted by the Company and/or the Group, that regulate and govern the Sensitive Activities covered by this Process are considered applicable:

○ Quality Manual. ○ Qualification of Supplier, Customer and Service Providers (UKUNK-WI-QA-0001). ○ Supply of the Product as an unlicensed medicine (UKUNK-SOP-QA-0001).

3.3 MANAGEMENT OF LEGAL AND CORPORATE AFFAIRS

Sensitive Activities

This Process includes – in particular – the following Sensitive Activities:

- ❖ Management of intercompany/infragroup relations/contracts.
- ❖ Litigation, settlements and legal advice.

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 24 *ter* - Law No. 146/2006 - Organised crime offences (incl. transnational);
- Art. 25 - Embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office;
- Art. 25 *ter* –Corporate offences;
- Art. 25 *octies* - Receiving stolen goods; money laundering; use of money, goods or benefits of unlawful origin; and self-laundering;
- Art. 25 *decies* - Inducement to make false statements to judicial authorities; and
- Art. 25 *quinquiesdecies* - Tax offences.

Rules of Conduct

In the performance of the Sensitive Activities referred to in this Process, all Addressees are required to observe the rules of conduct set out below:

Management of intercompany/infragroup relations/contracts

- Ensure that intercompany relationships are regulated through specific contracts, drafted in accordance with defined intra-Group standards - aimed at ensuring, among others, compliance also with regulations that are not of direct legal relevance (such as, for example, tax correctness of pricing, accounting transparency and asset separation) - and governing, among others:
  - the details of all contracted activities and services provided;
  - the roles and responsibilities of all parties; and
  - the agreed fees and relevant parameters for determining the fees.
- Ensure that contracts entered into with Group companies are signed by individuals with appropriate powers.
- Ensure the traceability of all transactions with Group companies through the archiving of all relevant documentation.
- Ensure that intercompany relations are based on the principles of fairness and transparency, in compliance with the principle of autonomy of the Group companies and the principles of proper management, so as to guarantee the protection of all stakeholders of Group companies.
- Preparation of adequate reporting to senior management regarding the new I/C agreements.

Litigation, settlements and legal advice

- Ensure that, in dealings with the judicial authorities, the competent corporate functions provide effective cooperation and make truthful, transparent and exhaustively representative statements of the facts.
- Ensure timely notification to the Company of summons received from the judicial authorities and of any subsequent developments in proceedings in which the individual called upon to make statements to the judicial authorities is involved as a person with the right to refuse to answer questions to allow the Company itself to take the appropriate measures aimed at ensuring the independence and autonomy of the individual in question and at the same time to protect the Company from potential risks in terms of the administrative liability of entities.

- Promptly inform the Company's management of any litigation involving (incl. potentially) the Company that it becomes aware of in the course of its activities.
- Ensure that, in their relations with the judicial Authorities, any individuals under investigation or charged in criminal proceedings (incl. related proceedings) in relation to work performed for the Company can freely express their representations of the facts or exercise the right not to answer questions granted by law.
- Ensure the absolute autonomy of any individual called upon to gives statements to the judicial authorities regarding the choice of lawyer, i.e., safeguard his independence and freedom in expressing himself before the judicial authorities.
- In the event of audits and inspections by judicial authorities:
  - prepare an internal report to ensure the traceability of all audits or inspections;
  - ensure the participation in these audits/inspections of at least two persons belonging to different corporate functions and endowed with appropriate powers;
  - email their contact persons concerning the outcome of the audit/inspection; and
  - in the event of findings by the judicial authorities, prepare a specific improvement plan by the person in charge or a person specifically appointed by them that identifies the nonconformities and/or irregularities observed by the inspectors during the visit and defines any corrective actions.
- Select external lawyers based on proven expertise in the field covered by the consultancy.
- Apply, where possible and appropriate, a principle of rotation of legal advisers, taking due account of the specific expertise of these professionals.
- Bind outside counsel with specific contractual clauses that stipulate: (a) compliance with the requirements set out in the Supplier Code of Interdependence and the Anti-Bribery Policy; and (b) the right of the Company, in the event of non-compliance, to unilaterally terminate the contract entered into and to claim compensation for any damage caused by breaches of the above requirements.
- Actively participate in the management of all activities carried out by external lawyers, including through periodic dialogue with external lawyers, timely sharing of documentation, participation in investigations and reviews of document drafts.
- Evaluate – in consultation with external lawyers – the legal actions to be taken (active or passive) to adopt the most appropriate strategy also in view of the nature, subject and value of the lawsuit.

- Request external lawyers to provide the Company's management a periodic report on the progress of litigation, possible development scenarios and any problems with the court decisions.
- Record outstanding disputes with the most material information (i.e., claimant, defendant, subject matter, amount claimed, legal representatives and status of the dispute).

In accordance with recent case law, in the event that the Company was identified as the accused entity in the context of proceedings pursuant to Decree 231 and in such proceedings the legal representative of the Company was directly involved as a suspect for the predicate offence of the administrative offence ascribed to the entity, the appointment of the Company's defence counsel must be made by a person other than (equipped with the appropriate powers) the said legal representative.

Prohibitions

In any case, it is forbidden to engage/collaborate/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. More specifically, for example, the following is forbidden:

Management of intercompany/infragroup relations/contracts

- Carrying out activities and/or operations aimed at creating false accounting records (e.g., through the use of invoices for non-existent transactions issued by third parties) aimed at creating advantages that could potentially be used to commit offences, with particular regard to corruption.
- fictitiously attribute the availability or ownership of money, goods or other utilities in order to circumvent legal provisions regarding patriotism prevention measures.

Litigation, settlements and legal advice

- Engage in conduct in violation of the law in formal and informal meetings, incl. through external lawyers and consultants, to induce the judicial authorities to unduly favour the interests of the Company.
- Engage in conduct in violation of the law during inspections/checks/audits by the judicial authorities to influence their judgement/opinion in the interest of the Company, also through external lawyers and consultants.

- Submit untruthful statements or documentation to the judicial authorities or their representatives to obtain undue advantages (e.g., gaining a favourable advantage in civil/criminal proceedings).
- Promise or pay money (incl. through third parties) to representatives of the judicial authorities, Public Administration (e.g., the GdF) or private individuals (e.g., legal advisors), also in a personal capacity or as a result of unlawful pressure, in particular to obtain undue advantages for the Company.
- Give or promise money or other benefits to intermediaries as consideration for their unlawful mediation whereby they exploit existing or alleged relations with public entities to exert an influence on the actions of the judicial authorities to the benefit of the Company.
- Make payments or recognise fees to third parties working on behalf of the Company that are not adequately justified in relation to the type of assignment contractually entrusted.
- Establish collaborative relations remunerated in any way with employees, collaborators or trainees of the judicial authorities and engage in conduct aimed at unduly influencing their judgement/opinion.
- Coerce or induce, in any form or way and in the interest of the Company, a decision of the Addressees to answer to the judicial authorities or to avail themselves of the right not to answer.
- Accept, in dealings with the judicial authorities, money or other benefits (incl. through Company Consultants).
- Promise or offer money or any other benefit, or resort to violence or threats, to induce a person called to testify not to make statements or to make false statements to the judicial authorities, if these statements could be used in a criminal trial.
- Make cash donations to Italian or foreign public officials either directly or through consultants or third parties acting in the name and on behalf of the Company.
- Grant advantages of any kind (promises of employment, etc.) to representatives of the judicial authorities that could influence the independence of judgement or induce them to secure an advantage for the Company.
- With regard to the management of disputes with private parties and the management of relations with arbitrators (in the context of the settlement of disputes through the appointment of an arbitrator or a board of arbitrators), it is forbidden to solicit/induce/receive, directly or through consultants or other third parties, an undue advantage (e.g., inducing the counterparty to settle in a manner favourable to the

Company) or accept an offer or promise to perform or refrain from performing an act in breach of one's legal, professional or contractual duties relating to the relevant activity (e.g., to settle in a way unfavourable to the Company).

- Inducing with gifts or promises of payment or other benefits persons called upon to make statements in proceedings to act in the interest or to the advantage of the Company.
- Make services or payments to external lawyers, consultants, experts or other third parties acting on behalf of the Company that are not adequately justified in the context of the contractual relationship established with them.
- Behave in a discriminatory and/or retaliatory manner towards a person called upon to make statements to the judicial authorities as a result of the statements made to the authority.

Specific checks

With specific regard to the *management of intercompany/intra-group relations/contracts*, the following controls are performed (by the head of the Legal Function of Chiesi Farmaceutici S.p.A. e Chiesi Ltd, to the extent of their responsabilities):

- ✓ Verification of the signing of contracts governing intercompany relationships by individuals with appropriate powers.

With specific regard to the *Management of Litigation, Settlement Agreements and Legal Advice*, the following checks are performed (by the Head of the Legal Function):

- ✓ Constant monitoring of active and passive criminal, civil, administrative and tax lawsuits.
- ✓ Monitoring the services performed by external lawyers to verify the way in which these activities are carried out.
- ✓ Verification that all documentation and deeds produced in the context of the management of disputes and relations with the judicial authorities are signed by individuals with appropriate powers.
- ✓ Verification of the signing of any proposals for settlement/arbitration agreements by individuals with appropriate powers.
- ✓ Verification of the absence of potential conflicts of interest between the professionals in charge of managing the litigation and the parties involved in the litigation/settlement agreement.
- ✓ Checks on the consistency of all fees paid to consultants/legal professionals with the activities actually carried out.

Procedural controls

In the performance of activities on behalf of UNIKERIS, Chiesi Farmaceutici S.p.A. applies – to the extent applicable – the relevant SOPs governing these activities.

3.4 INTELLECTUAL PROPERTY

Sensitive Activities

This Process includes – in particular – the following Sensitive Activity:

- ❖ Trademark and Patent Management (related to the Product).

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 25 - Embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office;
- Art. 25 *bis* - Counterfeiting money, public credit cards, revenue stamps or identification instruments or signs;
- Art. 25 *bis* 1 - Crimes against industry and trade; and
- Art. 25 *quinquesdecies* - Tax Offences.

Rules of conduct

In the performance of the Sensitive Activities referred to in this Process, all Addressees must observe the rules of conduct set out below:

- Strictly observe all laws and regulations governing the management of intellectual works.
- Promote the correct use of all intellectual works.
- Manage relations with licensees in compliance with current legislation, with an appropriate degree of formalisation, and in accordance with the principles of transparency and fairness.
- Regulate the methods for granting licences in compliance with the applicable laws and regulations.
- Adopt conduct that complies with the ethical principles adopted by the Group on tax policy.
- Make use of appropriate indemnification measures for any claims, lawsuits and compensation claims filed by third parties as a result of infringements of patents or patent

applications, trademarks or registered models and industrial and intellectual property rights relating to products purchased from third parties.

- Promptly inform the company management of any claims/legal proceedings/claims filed by third parties concerning the alleged unlawful use of intellectual works.
- Strictly observe tax obligations arising from the management of intellectual and industrial property rights, also with the support of specialised external consultants.
- Manage relations with the public authorities responsible for issuing/renewing trademarks and patents exclusively through individuals with appropriate powers and in full compliance with the law, current regulations, and the principles of transparency and fairness.
- In the management of communications with public authorities:
  - operate with fairness and impartiality through the corporate communication channels designated for that purpose;
  - represent the interests and positions of the Company in a truthful, transparent and consistent manner, avoiding any disclosure of untrue, incomplete or misleading information or statements to procure an undue advantage to the Company; and
  - if documentation to be submitted is produced with the full or partial support of third parties (consultants, technical experts, etc.), ensure that the selection of these parties is always carried out in compliance with the requirements of professionalism, independence and competence.
- In the event of non-compliance with requests by a representative of public authorities:
  - do not comply with the request; and
  - provide timely information to the company management.

Prohibitions

In any case, it is forbidden to engage/collaborate/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. More specifically, for example, it is forbidden to:

- unlawfully reproduce, imitate or tamper with trademarks, distinctive signs, patents, industrial designs or models owned by third parties;
- use, in an industrial and/or commercial context, trademarks, distinctive signs, patents, industrial designs or models counterfeited by third parties;
- use distinctive names or signs likely to create confusion with distinctive names or signs legitimately used by others, or falsify the products of a competitor, or perform by any

other means acts likely to produce confusion with the products and activity of a competitor;

- use, in any form or manner whatsoever, intellectual works that the Company does not hold exclusive ownership rights over and/or have legitimate title to use and whose existence could be discovered through ordinary and qualified diligence;
- engage in conduct, also with the help of third parties, aimed at falsifying or altering documentary evidence and/or registration documents supporting tax and/or fiscal declarations to obtain tax savings by altering the data relating to royalties received in relation to corporate brands;
- introduce into the territory of the State to trade, hold for sale or in any way put into circulation products with counterfeit or altered trademarks or distinctive signs by third parties;
- give or promise money or other benefits to intermediaries as consideration for their unlawful mediation whereby they exploit existing or alleged relations with public entities to influence the actions of competent public authorities to the benefit of the Company;
- establish collaborative relations remunerated in any way with employees, collaborators or interns of the competent public authorities and engage in conduct aimed at unduly influencing their judgements/opinions;
- promise or pay money, also through third parties, to representatives of competent public authorities or private individuals (e.g., consultants and patent agents), also in a personal capacity or as a result of unlawful pressure, in particular to obtain undue advantages; and
- conceal or destroy correspondence or any other documentation relating to the Sensitive Activity described in this Process.

Specific checks

Head of Corporate Intellectual Property Function - Patents and Global Trademarks, Domains & Brand Protection of Chiesi Farmaceutici S.p.A., within their respective areas of responsibility, carry out the following checks:

- ✓ Priority checks before proceeding with registrations/renewals at the competent offices, to avoid conflicting with trademarks/domains/patents that have already been filed.
- ✓ Legitimacy checks on the legitimate ownership of the trademark/trademark/patent by the transferor in the case of acquisitions or licences for use.
- ✓ Inclusion of provisions in specific categories of contracts that envisage the acquisition of products protected by intellectual property rights whereby the counterparty:

- certifies that he is the lawful owner of the economic exploitation rights over the trademarks, patents, distinctive signs, designs or models that are subject to the assignment or, in any case, that he has obtained authorisation from the lawful owners to allow their use by third parties or that they are the subject of free use;
- certifies that the trademarks, patents, distinctive signs, designs or models assigned or licensed for use do not infringe any third-party industrial property rights;
- undertakes to indemnify and hold the Company harmless from any damage or harm resulting from the untruthfulness, inaccuracy or incompleteness of this declaration;
- undertakes to comply with current legislation on copyright and intellectual property rights, as well as on the handling of privileged information (confidentiality and privacy clauses); and
- undertakes to respect the Supplier Code of Interdependence;

✓ Final approval by the Company's management to grant licences to third parties.

The Finance Function of Chiesi Ltd and/or the Tax Function of Chiesi Farmaceutici S.p.A., within their respective areas of responsibility, verify that the contractual forecasts for royalties correspond to the data represented in the tax returns.

3.5 INFORMATION TECHNOLOGY

Sensitive Activities

This Process includes the following Sensitive Activity in particular:

❖ Management and use of IT tools.

The information tools and related applications available to individuals carrying out activities on behalf of UNIKERIS are owned by other Group companies (e.g., Chiesi Farmaceutici S.p.A. and Chiesi Ltd.) and are managed in accordance with the methods and procedures established at corporate and/or Group level.

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 24 - Computer fraud to the detriment of the State or other public body (Art. 640*ter* of the Italian Criminal Code);
- Art. 24 *bis* - Computer crimes; and
- Art. 25 *novies* – Copyright infringement offences.

Rules of Conduct

In the performance of the Sensitive Activities referred to in this Process, all Addressees must observe the rules of conduct set out below:

- Operate in full compliance with the corporate provisions governing the security of IT systems.
- Use the assigned IT resources exclusively for the performance of their work.
- Refrain from any conduct that could compromise the security, confidentiality and integrity of the company's and other parties' information and data.
- Access information systems solely using identification codes assigned to the individual person and periodically changing the passwords by the prescribed deadlines.
- Activate any measure considered necessary to protect the computer system, preventing third parties from gaining access to it in the event of removal from the workstation.
- Take measures to protect legally effective electronic documents to be sent externally.
- Report to company management any computer security incidents, providing all the information and any documentation necessary for a proper assessment of the case.
- Only use properly licensed software.
- Respect the copyrights of third parties by using only original source code or source code for which specific authorisation has previously been obtained from the holder of the relevant rights.
- Ensure that servers are hosted in specially dedicated and secured premises and that access to these premises is restricted to authorised personnel only.
- Ensure that backups of data hosted on servers are saved on a regular basis and that the media is adequately secured, i.e., stored and protected (incl. by fireproof systems).
- Guaranteeing access to the company's information systems and management applications only to authorised individuals through the allocation of passwords and user IDs.
- Carefully guard their access credentials to the Company's information systems, preventing third parties from gaining knowledge of them.
- Use the company's IT resources in compliance with the security measures established by the Company (changing and keeping passwords, use of protection systems such as antivirus, etc.) and avoid conduct that could compromise their proper functioning or cause damage to third parties.

Prohibitions

In any case, it is forbidden to engage/collaborate/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. More specifically, for example, it is forbidden to:

- engage in conduct that could compromise the confidentiality and integrity of the Company's information and data and any other conduct aimed at overcoming or circumventing the protections of another person's corporate system;
- alter electronic documentation, public or private, for evidentiary purposes;
- unlawfully intercept, impede or interrupt computer or telematic communications;
- artificially modify or delete the content of communications relating to computer or telecommunications systems;
- procure, reproduce, disseminate, communicate or bring to the knowledge of third parties codes, passwords or other means of accessing another person's computer or telecommunications system protected by security measures, or provide indications or instructions enabling a third party to gain access to another person's computer system protected by security measures;
- procure, produce, reproduce, import, disseminate, communicate, hand over or, in any event, make available to others any equipment, devices or computer programs with the aim of unlawfully damaging a computer or telecommunications system, the information, data or programs contained therein or pertaining thereto, or of facilitating the total or partial interruption or alteration of its operation (this prohibition includes the transmission of viruses with the aim of damaging the information systems of competing entities);
- destroy, deteriorate, delete, alter or suppress information, data or computer programmes (this prohibition includes unauthorised intrusion into the information system of a competing company, with the aim of altering the latter's information and data);
- destroy, deteriorate, delete, alter or suppress information, data and computer programs relating to healthcare or otherwise of public interest; ;
- destroys, deteriorates, damages, erases, alters or suppresses information in order to render in whole or in part the computer or telematic systems of others unusable or seriously hinder their operation;
- engage in conduct of any nature whatsoever, within the scope of one's working activities and/or through the use of the Company's resources, likely to infringe the intellectual property rights of others;

- duplicate, import, distribute, sell, lease, disseminate/transmit to the public or possess for commercial purposes – or in any case for profit – any computer programs, databases, or works with literary, musical, multimedia, cinematographic or artistic content for which the obligations arising from copyright law and related rights have not been fulfilled;
- unlawfully duplicate an intellectual work (e.g., software or management applications) to exploit it without payment of the relevant licence;
- install unauthorised software or otherwise use unauthorised or unlicensed software on company computer equipment;
- undertake actions to overcome the protections applied to corporate information systems;
- disseminate – via telematic networks – an original work or part of it;
- illegally access the company's computer or telecommunications systems and/or those of public or private parties (e.g., competing companies), incl. for the purpose of unlawfully acquiring, altering or deleting data and/or information;
- gain unauthorised access to information systems used by the Public Administration to intervene in any way in the way in which anyone is not entitled to data, information or programmes, or to obtain and/or modify them, for the benefit of the Company;
- introduce into the territory of the State, hold for sale, put up for sale or in any case put into circulation – to make a profit – goods/works made by usurping the copyright or patents of third parties;
- use company assets and, in particular, company computer equipment, to commit or induce the commission of offences or to pursue any purpose that is against the law in force or that could constitute a threat to public order, the protection of human rights or morality; and
- conceal or destroy correspondence or any other documentation produced in connection with the Sensitive Activities referred to in this Process.

Specific checks

The IT Functions of Chiesi Farmaceutici S.p.A. and Chiesi Ltd carry out, within their areas of responsibility, the following checks when appropriate:

- ✓ Defining criteria and methods for creating passwords for access to the network, applications, corporate information assets and critical or sensitive systems (e.g., minimum password length, complexity rules and expiry date).
- ✓ Updates of passwords for access to information systems is required periodically, in accordance with current legislation.

- ✓ New users are activated based on predefined methods and the criteria and methods for assigning, changing and deleting user profiles are defined.
- ✓ Periodic checks are carried out on the current activity of accounts and, in the event of inactivity, accounts are blocked.
- ✓ The effective deactivation of credentials and of all active users for individuals terminating their employment with UNIKERIS are monitored, with particular regard also to persons outside the company.
- ✓ Protection mechanisms are provided, where necessary, for files relating to the activities carried out by UNIKERIS, such as passwords and conversion of documentation into non-editable formats.

Procedural controls

In the performance of activities on behalf of UNIKERIS, Chiesi Farmaceutici S.p.A. applies – to the extent applicable – all relevant SOPs governing these activities.

3.6 FINANCE AND TAXATION

Sensitive Activities

This Process includes the following Sensitive Activities in particular:

- ❖ Management of active electronic invoicing.
- ❖ Accounting management.
- ❖ Management of tax obligations arising from active invoicing activities (e.g., IRES, IRAP and 770).

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 24*bis* - Computer crimes;
- Art. 25 *ter* - Corporate offences;
- Art. 25 *octies* - Receiving stolen goods; money laundering; use of money, goods or benefits of unlawful origin; and self-laundering; and
- Art. 25 *quinquesdecies* - Tax offences.

Rules of conduct

When performing the Sensitive Activities referred to in this Process, all Addressees are required to observe the rules of conduct set out below:

- Ensure that the main tax-related regulatory changes are promptly disseminated to the staff involved in tax management and provide adequate training of tax personnel and constant updates on tax news to monitor the development of the relevant risks.
- Pay the utmost attention when carrying out activities with third parties (e.g., financial transactions) and intra-group activities (i.e., purchase and/or sale contracts; management of financial flows and investments) to identify and/or prevent any operations/situations likely to constitute any of the criminal offences under consideration.
- Comply with anti-money laundering regulations and report to the company's management any breaches of the relevant provisions that they become aware of in the course of their duties or that they otherwise become aware of.
- Comply with all obligations (in terms of declarations and payments) and deadlines set by tax legislation in the area of direct and indirect taxes.
- Keep and preserve correctly all tax-relevant accounting records.
- Correctly transpose tax-relevant bookkeeping data into annual and periodic tax returns.
- Correctly settle periodic taxes.
- Keep track of all offsets of tax credits recalled in tax returns or payments.
- Promptly regularise all irregularities detected in the course of checks carried out internally.
- Ensure the correct tax treatment of income components, deductions and allowances in accordance with tax regulations.
- Allow access to the remote banking system only to personnel with appropriate credentials to ensure the correct settlement of taxes in accordance with all powers of attorney in force.
- Restrict access to the Company's tax information system to individuals with the necessary authorisations and permissions.
- Ensure continuous alignment between the user profiles assigned and the roles held within the Company.
- Maintain clear, transparent, diligent and cooperative conduct in relations with the tax authorities and provide all data and information requested.
- Ensure that individuals in charge of dealing with the tax authorities and the financial police (*Guardia di Finanza*) in matters concerning the assessment and settlement of taxes carry out periodic reporting activities and activities that become necessary by virtue of contingent circumstances to ensure that individuals with the necessary powers can undertake the necessary corrective activities. More specifically, in the event of audits and inspections by the financial/tax authorities:

- ensure the participation in these audits/inspections of at least two individuals belonging to different corporate functions and endowed with appropriate powers;
- ensure the traceability of all audits or inspections through the preparation of an appropriate internal report or minutes;
- email their contact persons concerning the outcome of the audit/inspection; and
- in the event of findings, prepare a specific improvement plan that identifies the non-conformities and/or irregularities observed by the inspectors during the visit and defines possible corrective actions.

- In the management of communications with the financial/tax authorities:
  - operate, with fairness and impartiality through the corporate communication channels designated for that purpose;
  - represent the interests and positions of the Company in a truthful, transparent and consistent manner, avoiding any exposure of untrue, incomplete or misleading information or statements to procure an undue advantage to the Company; and
  - if documentation to be submitted is produced with the full or partial support of third parties (consultants, technical experts, etc.), ensure that the selection of these parties is always carried out in compliance with the requirements of professionalism, independence and competence.
- In the event of non-compliant requests by a representative of the tax authorities:
  - do not comply with the request; and
  - provide timely information to the Company's management.

Prohibitions

In any case, it is forbidden to engage/collaborate/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. More specifically, for example, it is forbidden to:

- make payments or recognise fees to third parties working on behalf of the Company that are not adequately justified in relation to the type of assignment contractually entrusted;
- make payments to any party that are not adequately justified in the contractual relationship;
- make transfers of money if there is a well-founded suspicion that this could expose the Company to the risk of money laundering, receiving stolen goods, use of money, goods or utilities of unlawful origin or self laundering (even as an accomplice);
- create funds against unjustified payments;

- open accounts or passbooks anonymously or in fictitious names and use accounts opened in foreign countries where this is not related to the underlying activity;
- transfer cash or hold/transfer bearer bank or postal passbooks or bearer securities in euro or foreign currencies for amounts, even fractional, that amount to or exceed the legal limits in force;
- accept cheques issued by individuals who are not debtors to the Company unless they have been contractually identified by the debtor;
- issue bank and postal cheques, excluding bank drafts, for amounts equal to or exceeding the legal limits in force that do not bear the name or company name of the payee and the non-transferability clause;
- make payments in cash, except for particular types of purchases falling under petty cash and in any case within the maximum amounts provided for by the regulatory limits in force and the company's document system;
- receive sums through transfers of cash or bearer bank or postal passbooks or bearer securities in euros or foreign currency, other than shares, when the value of the transaction, even if fractioned, amounts to or exceeds the regulatory limits in force;
- carry out any transaction that could obstruct the identification of the origin of the associated funds (e.g., giro transfers or the purchase of securities or financial instruments) without a justified reason;
- carry out activities and/or transactions aimed at creating non-accounting availabilities (e.g., through the use of invoices for non-existent transactions issued by third parties), with a view to creating advantages that could potentially be used to commit offences;
- carry out transactions (incl. with Group companies) to evade tax regulations as well as legal provisions regarding asset prevention measures or smuggling;
- record data that is false, incomplete or in any case likely to provide a partial or inaccurate description of the economic, financial or tax position of the Company or the Group as well as in order to conceal transactions aimed at fictitiously attributing to others the ownership or availability of money, goods or other utilities;
- alter or destroy financial and accounting documentation and information, e.g., through unauthorised access to the company's information systems or other actions suitable for the above purpose;
- fail to share data and information required by law concerning the economic or financial position of the company or the Group, incl. when intended for the supervisory authorities

to which the company's business is subject; or fail to promptly send this data or any documentation requested by the above authorities;

- engage in any conduct that obstructs the supervisory functions (incl. during inspections) by the Supervisory Authority;
- engage in any conduct – through the use of computer and/or telematic systems – aimed at evading, or allowing others to evade, income or value-added taxes, incl. from carrying out simulated transactions or using other fraudulent means;
- evade income or value-added taxes;
- use or issue invoices or other documents for non-existent transactions;
- declare fictitious liabilities/expenses or assets/revenues in invoices or other documents relating to income tax or value added tax for amounts lower than the actual amount;
- engage in objectively or subjectively simulated transactions, or otherwise make use of false documentation or other fraudulent means;
- allow third parties to evade income tax or value added tax;
- conceal or destroy any accounting records or documents whose retention is mandatory to report inaccurate income or turnover for the purpose of evading income tax or value added tax or allowing third parties to evade them;
- disclose in any annual income tax or value-added tax declarations assets/revenues for an amount lower than the actual amount or non-existent liabilities/expenses;
- prepare or communicate data that is false, incomplete or in any case likely to provide a partial or inaccurate description of the reality regarding the Company's economic, financial or tax position;
- carry out any transaction that could obstruct the identification of the origin of the money without justification;
- carry out transactions, including with Group companies, to evade tax regulations;
- submitting untrue financial and/or tax declarations or documentation to a public body or its representatives in order to obtain undue benefits; and
- illegally access information systems of the Public Administration with the aim of: (a) altering the operation and/or programs of the telematic system; (b) altering the data and information contained therein (tax declarations, attestations or self-certifications addressed to public bodies, documentation created with the aid of digital signature tools, documentation relating to the employment file sent to the relevant bodies INAIL, INPS, etc.); or (c) damaging and/or destroying the data contained therein.

Specific checks

The following checks are carried out by the head of the Tax Function of Chiesi Farmaceutici S.p.A. and by the head of Finance Function of Chiesi Ltd, within their areas of responsibility:

- ✓ Verify the legality, correctness, completeness, accuracy, consistency and appropriateness of accounting information.
- ✓ Verify the correct application of the relevant accounting principles, as well as current legislation, in the process of accounting for current and deferred taxes.
- ✓ Verify the completeness and correctness of the data used for calculating taxes, tax calculations and accounting records.
- ✓ Verify the activities and/or accounting operations carried out to prevent the creation of false accounting practices (e.g., reporting invoices for non-existent transactions issued by third parties) or aimed at the creation of 'black funds' or 'parallel accounts'.
- ✓ Monitor the evolution of relevant legislation in order to ensure compliance with new tax regulations and deadlines for communications, reports and fulfilments regarding the tax authorities to avoid delays and inaccuracies in their submission.
- ✓ Verify compliance with all deadlines and procedures laid down in applicable legislation for the preparation of periodic tax declarations and the consequent payment of income and value added tax.
- ✓ Approve tax declarations by the Legal Representative of the Company.

Procedural controls

In the performance of activities on behalf of UNIKERIS, Chiesi Farmaceutici S.p.A. applies – to the extent applicable – the relevant SOPs governing these activities.

3.7 NON-CORE PURCHASES

Sensitive Activities

This Process includes the following Sensitive Activity in particular:

- ❖ Purchase of services.

Predicate Offences

This Process is aimed at the prevention of the following Predicate Offense families:

- Art. 25 - Embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office;

- Art. 25 *ter* - Corporate offences;
- Art. 25 *octies* - Receiving stolen goods, money laundering, use of money, goods or benefits of unlawful origin and selflaundering;
- Art. 25 *quinquesdecies* - Tax offences.

Rules of Conduct

When performing the Sensitive Activities referred to in this Process, all Addressees must observe the rules of conduct set out below:

- Ensure that relations with Suppliers/Consultants are conducted in strict compliance with laws, regulations in force and principles of fairness, correctness, clarity and transparency.
- Create a specific register of Suppliers/Consultants to collect and census all relevant and necessary information for the performance of activities.
- Authorise orders/contractual relations only with Suppliers/Consultants with appropriate reliability, integrity and ethical requirements.
- If a conflict of interest arises, promptly report these circumstances to company management and refrain from intervening in the operational/decision-making process concerning the relationship with the Supplier/Consultant.
- Document the reasons behind the selection of each Supplier/Consultant and archive all relevant documentation.
- Adequately justify in writing any recourse to a "sole supplier" arising from specific requirements (exclusive know-how, technological constraints, emergencies, abandoned tenders, proven experience in the matter, etc.), as well as any further derogation from the ordinary procedures for signing and/or managing contracts with Suppliers/Consultants, which must in any case always be formally approved in accordance with the prescribed authorisation levels.
- Proceed with the evaluation of all offers received based on criteria marked by transparency and – as far as possible – the limitation of subjectivity criteria and the principle of rotation of Suppliers/Consultants.
- Ensure the traceability of the Supplier/Consultant selection process by archiving the relevant supporting documentation.
- Ensure that supplies are authorised, verified and signed by individuals with appropriate powers.
- Ensure that relations with Suppliers/Consultants are formalised through specific written agreements signed by individuals with appropriate powers.

- Bind the Supplier/Consultant through specific contractual clauses that envisage: (a) compliance with the requirements set out in the Supplier Code of Interdependence and/or the Anti-Bribery Policy; and (b) the Company's right, in the event of noncompliance, to unilaterally terminate the contract entered into and to claim compensation for any damage caused by the Supplier's conduct in breach of the above requirements.
- Include special clauses in contracts with Suppliers/Consultants that stipulate, among other things:
  - the liability of the Supplier/Consultant also for the actions of any sub-suppliers with respect to the rights of third parties;
  - that the company concerned declares that it has the authorisations required by law to carry out its activities; and
  - that the untruthfulness of the above declarations could constitute grounds for unilaterally termination of the contract;
- Specify in contracts with Suppliers/Consultants a description of the services due from the counterparty, the fees, and payment terms and conditions.
- Generate and issue purchase orders exclusively via the corporate system and in accordance with the document system in force to allow traceability.
- Accurately and promptly record all purchase transactions, verifying in advance that they have been authorised based on formalised authorisation powers.
- Accept only services that have been explicitly ordered and that in any case comply with the specifications under the purchase order.
- Ensure that all payments to Suppliers or contractors are made only if properly supported by contract or order or following a pre-defined internal authorisation process.
- Make payments to Suppliers/Consultants directly and exclusively to accounts in their respective names, which must be verified and entered in the company system in advance.

Prohibitions

In any case, it is forbidden to engage/collaborate/give rise to conduct that could fall within the types of offences considered for the purposes of Legislative Decree 231/2001. More specifically, for example, it is forbidden to:

- establish relations with individuals who refuse to or are reluctant to provide information relevant to their correct, effective and complete knowledge or who raise any suspicions. This includes suspicions that arise because of possible transactions in non-cooperative

jurisdictions or requests or offers for services that – even if abstractly advantageous for the Company – present signs of irregularity or potential breaches of laws and regulations governing the movement of capital and goods or tax or accounting;

- establish relations with Suppliers/Consultants if there is a well-founded suspicion that this could expose the Company to the risk of Offences being committed, e.g., in the event of news or well-founded suspicions of corrupt conduct, or actions involving or supporting terrorist or money laundering activities perpetrated by the Supplier/Consultant;
- perform services for Suppliers/Consultants that are not adequately justified in the context of the contractual relationship established with them, and pay them fees that are not adequately justified in relation to the type of assignment to be performed and the practices in force in the local area;
- bind the company with verbal orders/contracts;
- enter into contracts with Suppliers/Consultants that envisage making payments for services into accounts based in countries other than the country in which the Supplier has established its registered office/operational/commercial headquarters;
- make payments to Suppliers/Consultants that have not been contractually agreed;
- make payments in cash to numbered current accounts or accounts not in the name of the Supplier/Consultant or other than those provided for in the contract;
- make payments in countries other than the country of residence/ registered office/place of business/commercial office of the Supplier/Consultant;
- make payments that are not properly documented;
- give or promise money or other benefits to intermediaries as consideration for their unlawful mediation whereby they exploit existing or alleged relations with public persons to exert influence on decisions of the Public Administration to the benefit of the Company;
- offer, promise or disburse money or other benefits to a private party or a party reported by a private party or authorise anyone to directly or indirectly perform these activities outside the normal authorisation process;
- carry out activities and/or operations aimed at creating non-accounting advantages (e.g., through the use of invoices for non-existent transactions issued by third parties) or advantages that could potentially be used to commit offences, with particular regard to corruption; and

- conceal or destroy correspondence or any other documentation produced in connection with the Sensitive Activity referred to in this Process.

Specific checks

The Head of the Function requesting the service carries out the following checks:

- ✓ Compare multiple offers/quotations.
- ✓ Verify the technical and professional reliability of the Suppliers/Consultants, as well as the possession of the requirements of honourableness, professionalism, regularity of contributions and financial soundness.
- ✓ Verify the Supplier's/Consultant's possession of valid certifications: (i.e., ISO 9001, ISO 14001, OHSAS 18001 and Legality Rating) and/or membership of registers.
- ✓ Verify the Supplier's registration on the White List (for Suppliers to which this applies, e.g., transporters and disposers).
- ✓ Verify the existence of the specific authorisations of Suppliers/Consultants carrying out activities for which these authorisations are required.
- ✓ Require the Supplier/Consultant to issue a specific self-declaration concerning the nonexistence of prejudicial situations (involvement in investigations and/or convictions for offences under the Criminal Code, etc., as well as conflicts of interest with the Company).
- ✓ Assess potential conflicts of interest with the Supplier/Consultant.
- ✓ Verify the approval of purchase requests by individuals with appropriate powers.
- ✓ Ensure, where required by applicable internal procedures, that relations with Suppliers or Consultants/professionals are formalised through specific written agreements, signed by individuals with appropriate powers.
- ✓ Verify the adequacy of fees charged by Suppliers/Consultants in relation to the service and market conditions.
- ✓ Issue approvals for invoicing and subsequent payments only in cases where the supplies/performances are in accordance with the agreements with the Supplier/Consultant.
- ✓ Verify the regularity of payments to ensure that they fully match with the recipients/customers and the counterparties actually involved.

Procedural controls

When performing activities on behalf of UNIKERIS, Chiesi Farmaceutici S.p.A. applies – to the extent applicable – the relevant SOPs governing these activities.

5. INFORMATION FLOWS

For the purposes of effective supervision of the Model's implementation, the Addressees – because of their roles and responsibilities – must send information flows to the Supervisory Body concerning the performance of Sensitive Activities.

Process	Area / Corporate Function	Information Flow	Periodicity
Non-core purchases	Head of Requesting Function	Anomalies revealed during verification of invoices received	Per event
		List of services exceeding EUR 15,000	Annual
Legal and Corporate Affairs	Legal Function of Chiesi Farmaceutici S.p.A. or Chiesi Ltd, to the extent of their respective responsibilities	Measures and/or news concerning the existence of criminal proceedings, incl. against unknown individuals, relating to facts of interest to the Company	Per event
		Measures and/or news concerning the existence of significant administrative proceedings or civil disputes relating to requests or initiatives by independent authorities, the tax authorities, local authorities, contracts with the public administration, requests for and/or management of public funds	Per event
		Significant or atypical financial/corporate transactions that could be at risk of Offences	Per event

Process	Area / Corporate Function	Information Flow	Periodicity
		Requests for legal assistance forwarded to the Company by management for criminal or civil proceedings against them	Per event
		Any changes affecting the system of delegated powers adopted by the Company	Per event
		Any inspections carried out by public bodies (e.g., judiciary, Financial Police (*Guardia di Finanza*, GdF) and other authorities)	Per event
		Results of inspections carried out by external authorities (Revenue Agency (*AdE*), Financial Police (*GdF*), labour authorities, etc.) that result in significant findings or action plans being drawn up to address these findings	Per event
		Measures and/or news from police investigation bodies or any other authorities that indicate the existence of investigations or proceedings (incl. against unknown individuals) for offences under Legislative Decree 231/2001 that involve the Company or its Corporate Bodies, Collaborators, Consultants, Partners or Suppliers	Per event
		Information on the signing of intercompany contracts	Half-yearly

Process	Area / Corporate Function	Information Flow	Periodicity
		Information on extraordinary transactions within the Group involving the Company	Per event
		List of agendas for the meetings of the Board of Directors of the Company	Half-yearly
Finance and Taxation	Tax Function of Chiesi Farmaceutici S.p.A. and Finance Function of Chiesi Ltd, within their respective areas of responsibility	Any inspections by public bodies (financial and tax authorities, GdF, etc.).	Per event
		Any notifications from auditors concerning aspects that could indicate shortcomings in the system of internal controls, observations on the financial statements and/or reprehensible facts	Per event
		Reports by the Board of Statutory Auditors on any anomalies/criticalities encountered in the performance of its assessment and monitoring activities on the adequacy of the Company's organisational structure and internal control system	Per event
		Anomalies revealed during invoice verification	Per event
		Certificate of submission of tax returns	Annual
		Information on the use of tax credits as compensation for amounts exceeding EUR 50,000	Annual
		Copies of the approved annual accounts	Annual

Process	Area / Corporate Function	Information Flow	Periodicity
		Notifications of ongoing tax audits	Half-yearly
		Notifications of the results of tax audits	Half-yearly
Management of Product Marketing/Supplying Activities	Quality Function of Chiesi Ltd and/or Customer Service Function of Chiesi Farmaceutici S.p.A., within their respective areas of responsibility	Faults in the management of the customer qualification process	Per event
		Updates related to any organizational and/or business changes	Per event
		Stipulation of new service contracts or amendments to service contracts with suppliers for the management of the supply activities of the Product within the Italian territory	Per event
	IEO&CM Function at Chiesi Farmaceutici S.p.A.	Any inspections or requests for information by customs authorities	Per event
	Customer Service Function of Chiesi	Summary of public/private tenders in which the Company has participated	Half-yearly

Process	Area / Corporate Function	Information Flow	Periodicity
	Farmaceutici S.p.A.		
	IEO&CM Function at Chiesi Farmaceutici S.p.A.	Certification of tax compliance arising from importation activities	Half-yearly
Information Technology	Group IT Function	Information on possible anomalies in computer systems/tools	Per event
Intellectual Property	Chiesi Farmaceutici S.p.A.'s Corporate Intellectual Property - Patents and Global Trademarks, Domains & Brand Protection Function, within their respective	Any inspections or requests for information by trademark-/patent-granting authorities	Per event

Process	Area / Corporate Function	Information Flow	Periodicity
	areas of responsibility		
	Legal Function of Chiesi Farmaceutici S.p.A. or Chiesi Ltd, to the extent of their respective responsibilities	Details of variations/changes to inter-company licence agreements	Per event
Regulatory and Pharmacovigilance	Quality Function of Chiesi Ltd and Pharmacovigilance Function of Chiesi US, within their respective areas of responsibility	Any inspections by public bodies (regulatory authorities, independent administrative authorities, etc.).	Per event
		Summary of complaints/reports forwarded by a supplier to the competent function	Half-yearly

In any case, the O.d.V. is vested with all the powers under the Model to request at any time any information, data, documentation or news from the Addressees of the Model. The Recipients of the Model must promptly provide the O.d.V. with all material requested.

The principle also remains that all information, news and events that, under the Model, could be considered useful for performing the O.d.V.'s duties must be forwarded to the O.d.V. without delay.

Additionally, all Addressees involved in the performance of Sensitive Activities must promptly report all information concerning unlawful conduct relevant under the Decree that is based on precise and concordant elements of fact or any breach of the Model.

If any circumstances arise that are not expressly regulated by this Special Part and that lend themselves to doubtful interpretation and/or application that would entail derogations from the application of the Special Part, each Addressee must promptly notify the Supervisory Body of the occurrence of these circumstances. This notification must include an appropriate description of the conduct in question and a report of the matter.

UNIKERIS

Modello di organizzazione, gestione e controllo ex D. Lgs. 231/2001

PARTE GENERALE

N° VERSIONE	DATA	NOTE
01	**31 maggio 2023**	Prima emissione
02	**luglio 2023**	Seconda emissione
03	**12 aprile 2024**	Terza emissione
04	**giugno 2026**	Quarta emissione

DEFINIZIONI 5

CAPITOLO 1: IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA 8

DELLE PERSONE GIURIDICHE, SOCIETÀ ED ASSOCIAZIONI 8

1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento 8

1.2 L'adozione del "modello di organizzazione, gestione e controllo" quale 12

possibile esimente dalla responsabilità amministrativa 12

CAPITOLO 2: LA SOCIETÀ, IL GRUPPO, LA *GOVERNANCE* E L'ASSETTO 14

ORGANIZZATIVO 14

2.1 La Società 14

2.2 L'assetto organizzativo della Società 14

CAPITOLO 3: L'ADOZIONE DEL MODELLO 17

3.1 Obiettivi perseguiti con l'adozione del Modello 17

3.2 Ambito di applicazione del Modello 18

3.3 Elementi portanti e principi ispiratori del Modello 18

3.4 Adozione del Modello 19

3.5 L'approccio basato sul "rischio accettabile" 19

3.6 Struttura del Modello 20

3.7 Criteri di predisposizione del Modello 20

3.8 Destinatari del Modello 22

CAPITOLO 4: L'ORGANISMO DI VIGILANZA 22

4.1 Nomina dell'Organismo di Vigilanza 22

4.2 Requisiti di eleggibilità 22

4.3 Durata in carica 26

4.4 Funzione dell'Organismo di Vigilanza 27

4.5 Poteri dell'Organismo di Vigilanza....29
4.6 Regole di convocazione e di funzionamento....30
4.7 Reportistica dell'Organismo di Vigilanza....31
4.8 Flussi informativi nei confronti dell'Organismo di Vigilanza....31
4.9 Segnalazioni di condotte rilevanti ai fini del Modello....34
4.10 Obblighi di riservatezza....35
4.11 Raccolta e conservazione delle informazioni....35
CAPITOLO 5: LA DIFFUSIONE E LA FORMAZIONE....36
5.1 La diffusione....36
5.2 La formazione....36
CAPITOLO 6: IL SISTEMA DISCIPLINARE....38
6.1 Funzione del Sistema Disciplinare....38
6.2 Le condotte rilevanti....38
6.3 Le sanzioni....39
6.4 Misure nei confronti degli amministratori e dei procuratori....40
6.5 Misure nei confronti dei Sindaci....40
6.6 Misure nei confronti di Terze Parti....41
CAPITOLO 7: LE VERIFICHE SULL'ADEGUATEZZA DEL MODELLO....42
CAPITOLO 8: LE COMPONENTI DEL MODELLO....42
8.1 Gli elementi del Modello....42
8.2 Elementi organizzativi del Modello....42
8.3 I presidi generali di controllo....43
8.3.1 Il Codice di Condotta....43
8.3.2 La *Policy Anti-Bribery*....44
8.3.3 Sistema dei poteri....44

8.3.4 Segregazione 44
8.3.5 Tracciabilità e archiviazione 45
8.3.6 Sistema di gestione dei processi esternalizzati 45
8.3.7 Sistema di gestione e controllo dei flussi finanziari 46
8.3.8 Controlli e monitoraggio 46
8.3.9 Flussi informativi 46
8.3.10 Clausole contrattuali 47
8.4 Protocolli di controllo della Parte Speciale 47

DEFINIZIONI

- "Attività Sensibili": le attività svolte dalla Società esposte al rischio di commissione dei Reati.
- "CdA" o "Consiglio": il Consiglio di Amministrazione della Società.
- "Chiesi": Chiesi Farmaceutici S.p.A.
- "Collaboratori": coloro che agiscono in nome e/o per conto di UNIKERIS sulla base di un mandato ovvero coloro che collaborano con UNIKERIS in forza di un contratto di collaborazione di qualsiasi natura (fatta eccezione per i Consulenti e i *Partner*).
- Codice di Condotta: il Codice di Condotta adottato da Chiesi Farmaceutici S.p.A. e valido per tutto il Gruppo
- "Consulenti": qualunque persona fisica o società indipendente che lavora per conto di UNIKERIS e/o di una società del Gruppo con lo scopo di fornire un parere specialistico o servizi professionali di natura intellettuale, utilizzati da UNIKERIS e/o da una società del Gruppo.
- "Destinatari": coloro che sono indicati nel paragrafo 3.8 del presente Modello.
- "D. Lgs. 231/2001" o "Decreto": il Decreto Legislativo n. 231 dell'8 giugno 2001 e successive modifiche ed integrazioni.
- "Fornitori": fornitori di beni e servizi della Società, professionali e non, inclusi quelli di natura finanziaria.
- "Funzioni": tutte le funzioni aziendali e/o di Gruppo deputate allo svolgimento delle attività aziendali rilevanti ai fini del presente Modello.
- "Gruppo" o "Gruppo Chiesi": Chiesi Farmaceutici S.p.A. e tutte le relative filiali.
- "Linee Guida di Confindustria": le linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001 approvate da Confindustria, nell'ultima versione pubblicata nel mese di giugno 2021.
- "*Management*": i componenti del CdA, i preposti della sede secondaria e i responsabili delle principali Funzioni di Gruppo coinvolte nelle Attività Sensibili.

- "Modello" o "Modello 231": il modello di organizzazione, gestione e controllo previsto dal D. Lgs. 231/2001.

- "Organi Sociali": il Consiglio di Amministrazione e il Collegio Sindacale della Società.

- "Organismo di Vigilanza" o "Organismo" o "OdV": organismo (monocratico o collegiale) interno preposto alla vigilanza sul funzionamento e sull'osservanza del Modello e al relativo aggiornamento.

- "P.A." o "Pubblica Amministrazione": la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio a titolo esemplificativo, l'Autorità Giudiziaria, le Istituzioni e Pubbliche Amministrazioni italiane e straniere, nazionali e locali, l'Autorità Garante della Concorrenza e del Mercato, l'Agenzia Italiana del Farmaco ("AIFA"), il Garante per la protezione dei dati personali, l'Autorità per l'energia elettrica, il gas e il sistema idrico e le altre Autorità di vigilanza, italiane ed estere, o soggetti privati agli stessi equiparabili, nonché i relativi funzionari e organi interni.

- "*Partner*": controparti contrattuali della Società, sia persone fisiche sia persone giuridiche, con cui la Società addivenga ad una qualunque forma di rapporto di collaborazione contrattualmente regolato, ove destinati a cooperare con la Società nell'ambito delle Attività Sensibili.

- "*Policy Anti-Bribery*": la *Policy Anti-Bribery* del Gruppo Chiesi, formalmente adottata da UNIKERIS attraverso delibera del C.d.A. del 5 dicembre 2022.

- "Procedure aziendali": *policies*, *guidelines*, istruzioni operative, sop aziendali e/o di Gruppo rilevanti nello svolgimento delle Attività Sensibili.

- "Processi": aree aziendali di Attività Sensibili.

- "Prodotto": il prodotto farmaceutico distribuito dalla Società – anche per il tramite di altre società del Gruppo – e destinato alla prevenzione, cura e trattamento di malattie e patologie rare.

- "Protocolli di Controllo": le regole di comportamento, i divieti e i controlli finalizzati a prevenire, con riferimento a ciascun Processo, la commissione dei Reati Presupposto.
- "Pubblici Ufficiali": (i) chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa; (ii) chiunque agisca in qualità ufficiale in nome o per conto di (a) una Pubblica Amministrazione di uno Stato, a livello locale, nazionale o federale, (b)

un'agenzia, ufficio o organo dell'Unione Europea o di una Pubblica Amministrazione di uno Stato, (c) laddove previsto dalla normativa dello Stato di riferimento, un'impresa di proprietà, controllata o partecipata da una Pubblica Amministrazione di uno Stato, a meno che tale impresa non operi su normale base commerciale nel mercato di riferimento, ossia su una base sostanzialmente equivalente a quella di un'impresa privata, (d) un'organizzazione pubblica internazionale, quali ad esempio la Banca Europea per la Ricostruzione e lo Sviluppo, la Banca Internazionale per la Ricostruzione e lo Sviluppo, il Fondo Monetario Internazionale, la Banca Mondiale, le Nazioni Unite o l'Organizzazione Mondiale del Commercio o (e) un partito politico, un membro di un partito politico o un candidato a una carica politica, italiano o straniero; (iii) qualunque incaricato di un pubblico sevizio, da intendersi come un soggetto che, a qualunque titolo, presta un pubblico servizio (cioè un'attività che è disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima). Sono esclusi lo svolgimento di semplici mansioni di ordine e la prestazione di opera meramente materiale.

- "Reato/i" o "Reato/i Presupposto": qualunque dei reati richiamati dal D. Lgs. 231/2001.
- "Sistema dei Poteri": l'insieme delle deleghe e delle procure conferite nell'ambito della Società, nonché gli eventuali poteri di rappresentanza conferiti alle Terze Parti.
- "Sistema Disciplinare": sistema disciplinare facente parte del presente Modello.
- "*SpeakUp&BeHeard*": sistema di segnalazione del Gruppo Chiesi composto da una piattaforma dedicata (indipendente dai sistemi informativi della Società) e da una casella vocale.
- "Terze Parti": i soggetti terzi indipendenti che svolgono la loro attività fornendo beni e/o prestando servizi nell'interesse/vantaggio e/o in nome e per conto della Società in relazione alle Attività Sensibili disciplinate dal presente Modello. Rientrano nell'ambito delle Terze Parti anche i Consulenti, gli appaltatori, i Fornitori, gli eventuali intermediari e/o agenti e i *Partner* che svolgano la loro attività nell'interesse/vantaggio e/o in nome e per conto della Società e in relazione ad una o più Attività Sensibili.
- "UNIKERIS" o la "Società": UNIKERIS LIMITED con sede legale in Manchester M22 5LG (Regno Unito), 333 Styal Road e con sede secondaria in Parma (PR), Stradello Marche 6.

CAPITOLO 1: IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA DELLE PERSONE GIURIDICHE, SOCIETÀ ED ASSOCIAZIONI

1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento

1.1.1 La responsabilità ai sensi del Decreto Legislativo n. 231/2001

In data 4 luglio 2001 è entrato in vigore il Decreto Legislativo 8 giugno 2001, n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*".

Il Decreto ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia ha già da tempo aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

L'art. 5 del D. Lgs. 231/2001 sancisce la responsabilità della società qualora determinati reati (reati *c.d.* presupposto) siano stati commessi nel suo interesse o a suo vantaggio:

(a) da persone "**apicali**", ossia persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che esercitano, anche di fatto, la gestione e il controllo della stessa (ad esempio, amministratori e direttori generali);

(b) da persone "**sottoposte alla direzione o alla vigilanza**" di uno dei soggetti apicali indicati alla lettera precedente (e quindi tutti i dipendenti non dirigenti e le Terze Parti).

Pertanto, nel caso in cui da parte di queste persone venga commesso uno dei reati *c.d.* presupposto, alla responsabilità penale della persona fisica che ha materialmente commesso il reato si aggiunge - se ed in quanto siano integrati tutti gli altri presupposti normativi - anche la responsabilità "amministrativa" della società.

Tale disciplina mira, dunque, a coinvolgere gli enti nella punizione di taluni reati commessi nel loro interesse (nell'ottica della politica d'impresa adottata) o a loro vantaggio (al fine di conseguire un beneficio patrimoniale dalla commissione del Reato) [1] . Sotto il profilo

[1] Recenti orientamenti della Cassazione – richiamati anche dalle Linee Guida di Confindustria - evidenziano come nei reati colposi (reati in materia di salute e sicurezza e reati ambientali) l'interesse o il vantaggio debbano riferirsi anche all'inosservanza delle norme cautelari (es. nel risparmio di costi per la sicurezza ovvero nel

sanzionatorio, per tutti gli illeciti commessi è sempre prevista a carico della persona giuridica l'applicazione di una sanzione pecuniaria; per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi.

La responsabilità prevista dal Decreto si configura anche in relazione ai reati commessi all'estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato medesimo.

Inoltre, le fattispecie incriminatici previste dal Decreto, quand'anche integrate solo allo stadio del tentativo, generano per la società la responsabilità prevista dal Decreto. In particolare, l'art. 26, comma 1 del Decreto, stabilisce che, nei casi di realizzazione nella forma di tentativo dei delitti indicati, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre ne è esclusa l'irrogazione nei casi in cui la società, ai sensi dell'articolo 26 "*impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento*".

1.1.2 I Reati

La tipologia dei reati c.d. presupposto è molto ampia e include le seguenti fattispecie:

(i) indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24 del D. Lgs. 231/2001);

(ii) delitti informatici e trattamento illecito di dati (art. 24 *bis* del D. Lgs. 231/2001);

(iii) delitti di criminalità organizzata (art. 24 *ter* del D. Lgs. 231/2001)[2];

(iv) peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25 del D. Lgs. 231/2001);

---

potenziamento della velocità di esecuzione delle prestazioni o nell'incremento della produttività, sacrificando l'adozione di presidi antinfortunistici).

[2] Si precisa che la Società aderisce all'orientamento interpretativo in tema di individuazione del reato-base del delitto di associazione per delinquere secondo cui la responsabilità 231 dell'ente per i reati di cui al D. Lgs. 231/2001 deve essere circoscritta ai soli casi in cui la fattispecie contestata sia ricompresa in uno dei Reati Presupposto indicati nel Decreto stesso (si veda Cass. Pen. Sez. VI, n. 3635 del 24 gennaio 2014). Tale approccio

(v) reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 *bis* del D. Lgs. 231/2001);

(vi) delitti contro l'industria e il commercio (art. 25 *bis.*1 del D. Lgs. 231/2001)

(vii) reati societari (art. 25 *ter* del D. Lg. 231/2001);

(viii) reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 *quater* del D. Lgs. 231/2001);

(ix) reati relativi alle pratiche di mutilazione degli organi genitali femminili (art. 25 *quater.*1 del D. Lgs. 231/2001);

(x) reati contro la personalità individuale (art. 25 *quinquies* del D. Lgs. 231/2001);

(xi) reati e illeciti amministrativi di abuso di mercato (art. 25 *sexies* del D. Lgs 231/2001);

(xii) reati transnazionali (art. 10 della Legge 16 marzo 2006, n. 146);

(xiii) reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies* del D. Lgs. 231/2001);

(xiv) reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 *octies* del D. Lgs. 231/2001);

(xv) delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 *octies.*1 *ex* D.Lgs. 231/2001);

(xvi) delitti in materia di violazione del diritto d'autore (art. 25 *novies* del D. Lgs. 231/2001);

(xvii) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità di giudiziaria (art. 25 *decies* del D. Lgs. 231/2001);

(xviii) reati ambientali (art. 25 *undecies* del D. Lgs. 231/2001);

(xix) impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies* del D.Lgs. 231/2001);

(xx) delitti di razzismo e xenofobia (art. 25 *terdecies* del D. Lgs. 231/2001);

---

viene adottato dalla Società anche in relazione alla valutazione della fattispecie di autoriciclaggio, in linea con quanto chiarito dalle Linee Guida di Confindustria sul punto.

(xxi) frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 *quaterdecies* del D. Lgs. 231/2001);

(xxii) reati tributari (art. 25 *quinquiesdecies* del D. Lgs. 231/2001);

(xxiii) delitti di contrabbando (art. 25 *sexiesdecies* del D. Lgs. 231/2001);

(xxiv) delitti contro il patrimonio culturale (art. 25 *septiesdecies* del D.Lgs. 231/2001);

(xxv) riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 *duodevicies* del D.Lgs. 231/2001);

(xxvi) delitti contro gli animali (art. 25-*undevicies* del D.Lgs. 231/2001).

Tuttavia, **non tutti i Reati Presupposto sono effettivamente ipotizzabili** in relazione all'attività aziendale della Società. Nella **Parte Speciale del Modello** verranno specificamente indicati i Reati che sono stati considerati potenzialmente rilevanti nell'espletamento delle attività aziendali.

1.1.3 Applicabilità del D.Lgs. 231/2001 agli enti di diritto straniero

L'art. 1, co. 2, D.Lgs. n. 231/2001 definisce l'ambito di applicazione della disciplina in materia di responsabilità amministrativa degli enti senza delineare alcuna distinzione fra enti aventi sede in Italia e enti aventi sede all'estero.

Sin dall'inizio, la giurisprudenza di merito si è espressa sostenendo che poiché il criterio che radica la competenza a decidere sulla responsabilità amministrativa dell'ente, ai sensi dell'art. 36, comma 1, D.Lgs. n. 231/2001, è quello del c.d. *locus commissi delicti*, ossia del luogo ove è stato commesso il reato presupposto, anche una persona giuridica con sede principale all'estero può essere indagata qualora il reato presupposto sia stato commesso in Italia.

Inoltre, secondo recenti orientamenti giurisprudenziali[3] non vi è "*ragione alcuna per ritenere che le persone giuridiche siano soggette ad una disciplina speciale rispetto a quella vigente per le persone fisiche sì da sfuggire ai principi di obbligatorietà e di territorialità della legge penale*". Infatti, gli artt. 3 e 6, co. 1, c.p. dispongono che (i) la legge penale italiana sia obbligatoria nei confronti di tutti coloro che si trovino nel territorio italiano, a prescindere dalla loro nazionalità, e fatte salve le eccezioni del diritto pubblico e del diritto internazionale, e che (ii) il reato commesso nel territorio italiano sia punito secondo la legge italiana.

[3] *Cfr.* Cassazione Penale, sez. VI, sentenza n. 11626 del 7 aprile 2020 (conforme, Cassazione Penale, sez. IV, sentenza n. 32899, dell'8 gennaio 2021 - dep. 6 settembre 2021).

Dunque, la commissione del Reato Presupposto – in tutto o in parte – nel territorio italiano comporta l'applicabilità del D.Lgs. 231/2001 nei confronti dell'ente nel cui interesse o vantaggio il Reato è stato commesso, a nulla rilevando il fatto che l'ente abbia la propria sede principale in un altro Paese, né che la legge di tale Paese non preveda oneri di carattere organizzativo-preventivo analoghi a quelli del D.Lgs. 231/2001.

1.2 L'adozione del "modello di organizzazione, gestione e controllo" quale possibile esimente dalla responsabilità amministrativa

L'articolo 6 del Decreto introduce una particolare forma di esonero dalla responsabilità in oggetto qualora la società dimostri:

(a) di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del fatto, un modello di organizzazione e controllo idoneo a prevenire reati della specie di quello verificatosi;

(b) di aver affidato ad un organismo interno, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del modello, nonché di curarne l'aggiornamento;

(c) che le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il suddetto modello;

(d) che non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Il Decreto (così come modificato dal D.Lgs. n. 24/2023[4]) prevede, inoltre, che il modello di organizzazione e controllo – in relazione all'estensione dei poteri delegati e al rischio di commissione dei Reati – debba rispondere alle seguenti esigenze:

1. individuare le attività nel cui ambito esiste la possibilità che vengano commessi i Reati (*c.d.* Attività Sensibili);
2. prevedere, o fare rinvio a specifici protocolli che regolino la formazione e l'attuazione delle decisioni aziendali in relazione ai Reati da prevenire;
3. individuare le risorse finanziarie idonee ad implementare un sistema di organizzazione tale da prevenire la commissione dei Reati;

[4] D.Lgs. n. 24/2023 "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*".

4. prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del modello;

5. configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;

6. prevedere i canali di segnalazione interna e il divieto di ritorsione di cui al D.Lgs. n. 24/2023 ("**Decreto 24/23**");

7. prevedere nel sistema disciplinare di cui al precedente punto 5 sanzioni nei confronti di chi (i) viola le misure di tutela del segnalante, delle persone coinvolte e delle persone menzionate nella segnalazione di cui all'art. 12 del Decreto 24/23; (ii) adotta azioni ritorsive nei confronti del segnalante (e/o degli ulteriori soggetti di cui all'art. 3, comma 5, del Decreto 24/23[5]), per motivi collegati, direttamente o indirettamente, alla segnalazione; (iii) ostacola o ha tentato di ostacolare le segnalazioni.

[5] Ai sensi dell'art. 3, comma 5, del Decreto 24/23, le misure di tutela dagli atti ritorsivi indicati all'art. 17 del Decreto 24/23 si applicano: ai segnalanti (i.e. soggetti sia interni che esterni all'azienda e legati a questa da un rapporto di lavoro e/o collaborazione, così come definiti all'art. 3 del Decreto 24/23); ai facilitatori dei segnalanti; alle persone del medesimo contesto lavorativo del segnalante e legate a lui/lei da uno stabile legame affettivo o di parentela entro il quarto grado; ai colleghi di lavoro del segnalante, che lavorano nello stesso contesto lavorativo del segnalante e che hanno con lui/lei un rapporto abituale e corrente; agli enti di proprietà del segnalante o per i quali il segnalante lavora, nonché agli enti che operano nel medesimo contesto lavorativo del segnalante.

CAPITOLO 2: LA SOCIETÀ, IL GRUPPO, LA *GOVERNANCE* E L'ASSETTO ORGANIZZATIVO

2.1 La Società

UNIKERIS LIMITED è una società di diritto inglese con sede legale in Manchester M22 5LG (Regno Unito), 333 Styal Road che ha istituito a partire dal 1° gennaio 2022 una propria sede secondaria italiana in Parma (PR), Stradello Marche 6. La Società è fiscalmente residente in Italia.

La principale attività della Società è la distribuzione del Prodotto. Attualmente, la Società distribuisce, tramite le società del Gruppo o terzi (tra cui *Partner* e Terze Parti), il Prodotto ad enti ospedalieri in diverse aree geografiche (es. Europa, Turchia, *Middle East* e Giappone). Il Prodotto è autorizzato negli Stati Uniti d'America e in Giappone.

2.2 L'assetto organizzativo della Società

Il capitale sociale della Società è interamente posseduto da Chiesi Farmaceutici S.p.A. che pertanto è il socio unico della Società.

La sua forma giuridica è quella della società unipersonale privata per azioni e il suo sistema di *governance* è composto da Assemblea dei soci, Consiglio di Amministrazione e Collegio Sindacale.

2.2.1 Assemblea dei soci

Le deliberazioni assunte dall'Assemblea dei soci devono essere ordinarie o speciali in conformità alla normativa applicabile. In particolare, l'approvazione del bilancio annuale della Società, la nomina e la revoca degli amministratori, la nomina del Collegio sindacale e del suo Presidente, e di qualsiasi persona o ente incaricato della revisione legale dei conti della Società, la determinazione della remunerazione degli amministratori e dei sindaci, qualsiasi deliberazione sulla responsabilità degli amministratori e dei sindaci dovranno essere approvate con deliberazione ordinarie. Le modifiche allo statuto, lo scioglimento della società, la nomina dei liquidatori ed ogni altra materia ai sensi di legge o dello statuto dovranno essere approvate con deliberazione speciale.

L'Assemblea è presieduta dal Presidente del Consiglio di Amministrazione.

2.2.2 Amministratori

All'organo amministrativo è affidata la gestione della Società e a tal fine l'organo può compiere tutti gli atti e tutte le operazioni sia di ordinaria che di straordinaria amministrazione, con la sola esclusione di quegli atti e di quelle operazioni che la legge e/o lo statuto riservano espressamente ai soci.

Attualmente l'organo amministrativo ha la forma di Consiglio di Amministrazione composto da cinque membri, a maggioranza italiana. Inoltre, l'organo amministrativo ha nominato Tre dei membri del Consiglio di Amministrazione come "institori" attribuendolo loro tutti i poteri relativi alla gestione della sede secondaria della Società ai sensi degli articoli dal 2203 al 2208 inclusi del codice civile italiano, da esercitarsi disgiuntamente e con la facoltà di sub- delegare a terzi singoli atti o categorie di atti.

La rappresentanza legale della Società spetta al Presidente del Consiglio di Amministrazione; la rappresentanza sociale spetta anche agli institori nei limiti dei poteri determinati nell'atto di nomina.

Nel caso di attribuzione di deleghe a più amministratori, con poteri congiunti e/o disgiunti, la rappresentanza legale spetta anche agli stessi, coerentemente con i poteri delegati.

2.2.3 Collegio sindacale

Il Collegio sindacale ha il compito di vigilare (i) che l'organo amministrativo e l'assemblea degli azionisti adempiano alla legge e allo statuto e (ii) sull'osservanza dei principi di corretta amministrazione e sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile.

Il Collegio sindacale può (i) compiere atti di ispezione e di controllo e (ii) richiedere informazioni agli amministratori sull'andamento della gestione sociale o su determinati affari.

2.2.4 Organizzazione

La Società ha dimensioni ridotte; tutte le principali decisioni gestionali e commerciali relative all'attività della Società sono adottate in Italia.

Le attività aziendali sono esternalizzate, mediante appositi contratti a (i) soggetti terzi (tra cui Terze Parti) e (ii) altre società del Gruppo (con il supporto di specifiche Funzioni aziendali).

Con riferimento all'esternalizzazione delle attività aziendali *sub.* i), le Terze Parti svolgono nei confronti della Società, a titolo esemplificativo e non esaustivo, attività relative alla distribuzione del Prodotto, gestione ed evasione degli ordini del Prodotto, partecipazione alle procedure indette dalla Pubblica Amministrazione per la fornitura del Prodotto.

Invece, relativamente all'esternalizzazione delle attività aziendali *sub.* ii), le società del Gruppo Chiesi primariamente coinvolte sono (a) Chiesi Limited che, tramite funzioni/dipendenti con

sede in *UK*, fornisce alla Società una serie di servizi (es. servizio clienti, servizi di collegamento medico, affari medici, direzione, servizi finanziari, consulenza e assistenza per tutte le questioni relative alla gestione delle risorse umane, servizi legali, servizi di segreteria societaria, servizi di supporto e servizi normativi e garanzia della qualità) e (b) Chiesi Farmaceutici S.p.A. che, tramite funzioni/dipendenti con sede in Italia, fornisce servizi di supporto manageriale, la gestione degli adempimenti in materia fiscale relativi alla sede secondaria e di proprietà intellettuale.

L'allocazione delle attività in capo a Chiesi Farmaceutici S.p.A. consente di far rientrare l'attività della Società nella più ampia strategia del Gruppo Chiesi e di standardizzare la gestione del portafoglio prodotti aziendale e dei diritti di proprietà intellettuale del gruppo Chiesi.

CAPITOLO 3: L'ADOZIONE DEL MODELLO

3.1 Obiettivi perseguiti con l'adozione del Modello

L'adozione del Modello è stata promossa in coerenza con i principi etici e di *governance* del Gruppo sulla base dei quali viene assicurata la conduzione delle attività, allo scopo di poter prevenire la commissione di particolari tipologie di reati, come specificamente prescritto dal decreto sopra richiamato.

La Società è consapevole del valore che può derivare da un sistema di controllo interno idoneo a prevenire la commissione dei Reati da parte dei propri Organi Sociali e, in genere, da parte dei terzi che operano in nome o per conto o comunque nell'interesse della Società, sotto la vigilanza dei soggetti apicali. Inoltre, la Società è consapevole che l'adozione e l'efficace attuazione del Modello migliorano il sistema di *Corporate Governance* in quanto limitano il rischio di commissione dei Reati e consentono di beneficiare dell'esimente prevista dal D. Lgs. 231/2001.

La predisposizione ed attuazione del Modello sono state effettuate nella convinzione che le stesse – al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio – possano costituire, oltre che una circostanza esimente ai sensi della disciplina italiana della responsabilità degli enti per gli illeciti amministrativi dipendenti da reato contenuta nel D. Lgs. 231/2001, un fondamentale strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto di UNIKERIS, affinché seguano, nell'espletamento delle proprie attività a favore della Società, dei comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei Reati.

Pertanto, scopo del presente Modello è la predisposizione di un sistema di prevenzione, dissuasione e controllo per la riduzione del rischio di commissione dei Reati mediante l'individuazione delle Attività Sensibili, dei principi di comportamento che devono essere rispettati dai Destinatari del Modello, nonché di specifiche attività di controllo, tutte finalizzate a prevenire la commissione dei Reati.

In particolare, il Modello si propone come finalità quelle di:

- sviluppare in tutti coloro che operano nell'ambito delle Attività Sensibili la consapevolezza di poter determinare - in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre norme e procedure aziendali (oltre che alla legge)illeciti passibili di conseguenze penalmente rilevanti non solo per sé stessi, ma anche per la Società;

- ribadire che tali forme di comportamento illecito sono fortemente condannate dalla Società in quanto (anche nel caso in cui la stessa fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali del Gruppo;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle Attività Sensibili, di intervenire tempestivamente per prevenire o contrastare la commissione dei Reati.

3.2 Ambito di applicazione del Modello

Il presente Modello 231 riguarda tutte le attività svolte dalla Società che saranno individuate come potenzialmente a rischio di commissione dei reati previsti dal Decreto 231 (*c.d.* Attività Sensibili).

È molto importante sottolineare che **il Modello copre anche le Attività Sensibili che sono in tutto o in parte affidate a Terze Parti o ad altre società del Gruppo**. Le principali Attività Sensibili in tutto o in parte affidate a Terze Parti o ad altre società del Gruppo sono indicate nella Parte Speciale.

In questo caso, i soggetti a cui sono affidate queste attività devono attenersi anch'essi a tutte le applicabili prescrizioni di questo Modello.

3.3 Elementi portanti e principi ispiratori del Modello

Devono considerarsi quali punti cardine del Modello:

- l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- la mappatura delle Attività Sensibili;
- la prevenzione del rischio, attraverso l'adozione di principi procedurali specifici volti a disciplinare la formazione e la corretta attuazione delle decisioni societarie in relazione ai Reati da prevenire;
- i presidi di controllo finalizzati alla prevenzione del rischio di commissione di Reati (in particolare, la verifica e documentazione delle operazioni poste in essere nell'ambito delle Attività Sensibili, il rispetto del principio della segregazione dei ruoli nella strutturazione dei processi aziendali e nelle attività di gestione delle risorse finanziarie, la definizione di poteri autorizzativi coerenti con le responsabilità assegnate e la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico (controllo *ex post*);

- l'attribuzione all'OdV di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello.

In particolare, il Modello **tiene conto dei processi e dei sistemi di controllo aziendali e di Gruppo esistenti e già operanti**, nella misura in cui essi siano considerati idonei a valere anche come misure di prevenzione dei Reati e di controllo sui processi coinvolti nelle Attività Sensibili.

Il Modello 231 è caratterizzato da: (i) efficacia, ossia adeguatezza dell'insieme dei controlli istituiti a prevenire la commissione di reati-presupposto; (ii) specificità, ossia considerazione delle caratteristiche, delle dimensioni, del tipo di attività e delle vicende storiche della Società; (iii) attualità, ossia costante aggiornamento.

Il disegno del Modello è stato improntato anche ad un criterio di proporzionalità nell'ambito del quale si sono stabilite regole e controlli proporzionati alle ridotte dimensioni e all'articolazione semplificata della struttura organizzativa della sede secondaria della Società, nonché delle esigenze di efficace diffusione del Modello a tutti i Destinatari.

3.4 Adozione del Modello

La presente Parte Generale del Modello è stata adottata per la prima volta in data 31.05.2023 con decisione del CdA. Con la medesima decisione è stato nominato l'Organismo di Vigilanza a cui è attribuito il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di promuoverne l'aggiornamento.

3.5 L'approccio basato sul "rischio accettabile"

Essenziale nella costruzione di un sistema di controllo preventivo è il concetto di "**rischio accettabile**". Nello specifico, ai fini dell'applicazione del D.Lgs. 231/2001, è fondamentale che sia definita una soglia effettiva che consenta di porre un limite alla quantità e qualità delle misure di prevenzione da adottare e attuare per evitare la commissione dei reati-presupposto. In assenza di una preventiva determinazione del rischio accettabile, la quantità/qualità di controlli preventivi istituibili sarebbe infatti virtualmente infinita, con intuibili conseguenze in termini di operatività aziendale. Lo stesso principio generale, invocabile anche nel diritto penale, dell'esigibilità concreta del comportamento costituisce in proposito un criterio di riferimento centrale.

Come evidenziato dalle Linee Guida di Confindustria con riferimento al sistema di controllo preventivo da costruire in relazione al rischio di commissione dei reati-presupposto, con riguardo ai reati dolosi la soglia concettuale di accettabilità è costituita da un sistema di

prevenzione tale da non poter essere aggirato se non fraudolentemente, in linea con la logica della "elusione fraudolenta" del Modello 231 quale esimente espressa ai fini dell'esclusione della responsabilità dell'ente (v. art. 6, comma 1, lett. c, del D.Lgs. 231/2001: "*le persone hanno commesso il reato eludendo fraudolentemente i modelli…*").

Come evidenziato in giurisprudenza, la "frode" a cui fa riferimento il D. Lgs. 231/2001 non richiede necessariamente veri e propri artifici e raggiri; al tempo stesso la frode non può però nemmeno consistere nella mera violazione delle prescrizioni contenute nel Modello 231. Essa presuppone che la violazione del Modello 231 sia determinata comunque da un aggiramento delle misure di sicurezza idoneo a forzarne l'efficacia.

In base a questi principi, per tutte le Attività Sensibili considerate "a rischio" di reati-presupposto, il Modello della Società è stato costruito avendo come obiettivo la definizione di una Parte Speciale che sia ragionevolmente in grado di impedire tutti i possibili reati dolosi, se non previa elusione fraudolenta.

3.6 Struttura del Modello

Le principali componenti del Modello 231 sono le seguenti:

(a) la presente Parte Generale, che illustra l'impianto complessivo del Modello 231 e l'insieme delle regole e dei principi generali dettati dal medesimo;

(b) la Parte Speciale, che regolamenta i processi aziendali e le Attività Sensibili e prevede le regole di comportamento, i divieti e i presidi di controllo per prevenire la commissione dei Reati.

3.7 Criteri di predisposizione del Modello

3.7.1 Fasi

Nella predisposizione del presente Modello la Società si è ispirata alle Linee Guida di Confindustria. Coerentemente con queste linee guida la predisposizione del Modello è basata su:

- individuazione dei processi aziendali e delle Attività Sensibili, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;
- predisposizione dei protocolli di controllo in grado di prevenire i rischi individuati.

La predisposizione del presente Modello (così come ogni successivo aggiornamento, qualora gli interventi abbiano carattere sostanziale) è peraltro integrata dalle seguenti attività:

3.7.1.1 Mappatura delle aree a rischio

Durante tale fase viene effettuata un'analisi del contesto aziendale, al fine di mappare tutte le attività svolte dalla Società e, tra queste, individuare quelle nel cui ambito possano essere astrattamente realizzati i Reati (*c.d.* Attività Sensibili).

L'individuazione delle Attività Sensibili viene effettuata attraverso l'esame preliminare della documentazione aziendale rilevante - tra cui a titolo esemplificativo: visura camerale, sistema di deleghe e procure, procedure aziendali e contratti - e la raccolta di informazioni dai soggetti in posizione apicale e dalle Funzioni del Gruppo.

Congiuntamente all'individuazione dei rischi potenziali, si procede con l'analisi del sistema di controllo adottato dalla Società che possa essere considerato rilevante ai fini della prevenzione dei rischi di commissione dei Reati considerati.

3.7.1.2 "*Gap analysis*"

Sulla base dei risultati ottenuti dall'analisi sopra descritta, la Società individua le azioni da attuare nell'ambito delle diverse Attività Sensibili (*gap analysis*), sia a livello di procedure interne e controlli esistenti, che di requisiti organizzativi al fine di pervenire alla definizione del Modello.

3.7.1.3 Modifiche, aggiornamento e miglioramento continuo del Modello

Le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del CdA. È peraltro riconosciuta al Presidente del CdA la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere non sostanziale. In entrambe le ipotesi, le suddette modifiche dovranno essere comunicate all'Organismo di Vigilanza.

In particolare, si procederà prontamente: (a) alla modifica del Modello ove siano ravvisate significative violazioni o elusioni dello stesso che ne mostrino l'inadeguatezza, anche solo parziale, a garantire l'efficace prevenzione dei reati-presupposto; (b) all'aggiornamento del Modello 231, anche su proposta dell'Organismo di Vigilanza, ove si verifichino rilevanti cambiamenti o modifiche nel sistema normativo e regolamentare, anche interno, che disciplina l'attività della Società e/o nella struttura, organizzazione o attività della stessa. Per i fini di cui sopra, l'Organismo di Vigilanza dovrà segnalare per iscritto all'organo amministrativo le circostanze che suggeriscono la necessità, o anche solo l'opportunità, di modificare o aggiornare il Modello 231.

3.7.2 Metodologia adottata per la predisposizione della Parte Speciale del Modello

La Parte Speciale del Modello è composta da specifici protocolli di controllo applicabili ai singoli processi aziendali e Attività Sensibili, per la cui predisposizione si è stabilito di seguire la metodologia descritta al § *I. Premessa* della stessa Parte Speciale, a cui si fa rinvio.

3.8 Destinatari del Modello

Le regole contenute nel presente Modello si rivolgono a tutte le persone che fanno parte dell'organizzazione della Società e in particolare:

(a) alle persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società;

(b) alle persone che esercitano, anche di fatto, la gestione ed il controllo della Società stessa;

(c) alle altre Funzioni aziendali e/o di Gruppo che svolgono attività per conto e/o nell'interesse della Società.

Inoltre, i principi di comportamento contenuti nel Modello e alcune regole specifiche si applicano anche alle Terze Parti.

CAPITOLO 4: L'ORGANISMO DI VIGILANZA

4.1 Nomina dell'Organismo di Vigilanza

Il Decreto, all'art. 6, comma primo, lett. b), pone come condizione per un idoneo Modello 231 che sia affidato ad un organismo della Società, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei modelli nonché di curarne l'aggiornamento.

In attuazione di questa prescrizione, la Società ha nominato il proprio Organismo di Vigilanza.

La nomina dell'Organismo di Vigilanza avviene mediante apposita delibera del CdA: a tal riguardo, al momento della nomina dovranno essere forniti nel corso della relativa riunione adeguati chiarimenti in merito alla professionalità dei suoi componenti.

Dell'avvenuta nomina dell'Organismo di Vigilanza è data comunicazione a tutti i componenti degli Organi Sociali.

4.2 Requisiti di eleggibilità

I componenti dell'OdV devono possedere adeguati requisiti di autonomia, indipendenza, professionalità, continuità di azione, oltre che di onorabilità ed assenza di conflitti di interesse.

4.2.1 Autonomia e indipendenza rafforzati

Il requisito di autonomia e indipendenza presuppone che l'OdV risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (organo amministrativo).

L'autonomia e l'indipendenza vanno intese in senso non meramente formale: è necessario cioè che l'OdV sia dotato di effettivi poteri di ispezione e controllo e che abbia possibilità di accedere di propria iniziativa alle informazioni aziendali rilevanti, che sia dotato di risorse adeguate e possa avvalersi di strumentazioni, supporti ed esperti nell'espletamento della sua attività di monitoraggio.

In particolare, tale requisito è assicurato dall'obbligo, in capo all'organo amministrativo, di approvare una dotazione annua adeguata di risorse finanziarie, anche su proposta dell'OdV stesso, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri doveri (es. consulenze specialistiche, eventuali trasferte, etc.).

L'indipendenza presuppone inoltre che l'OdV non si trovi in una posizione, neppure potenziale di conflitto d'interessi con la Società, né sia titolare all'interno della stessa di funzioni di tipo esecutivo che ne minerebbero l'obiettività di giudizio nel momento delle verifiche sul rispetto del Modello.

Infine, allo scopo di garantire i requisiti di indipendenza e di autonomia, dal momento della nomina e per tutta la durata della carica, l'OdV:

(a) non deve rivestire il ruolo di amministratore;

(b) non deve risultare titolare, direttamente o indirettamente, di partecipazioni nel capitale della Società né essere titolare, direttamente o indirettamente, di partecipazioni azionarie di entità tale da permettere di esercitare il controllo o un'influenza notevole sulla Società;

(c) se esterno alla Società, non deve intrattenere - direttamente o indirettamente - con la Società, né con società da essa controllate o ad essa collegate, relazioni economiche di rilevanza tale da condizionarne l'autonomia di giudizio, valutata anche con riferimento alla condizione patrimoniale soggettiva della persona fisica, né intrattenere significativi rapporti d'affari con gli amministratori muniti di deleghe (amministratori esecutivi) e con gli azionisti che controllano la Società;

(d) se interno alla Società, deve ricoprire un ruolo non esecutivo e non essere impegnato direttamente nelle attività di *business*, come ad esempio le persone impegnate nelle funzioni di *compliance* e/o di *internal audit*;

(e) può essere un soggetto che riveste la qualità di Sindaco;

(f) non deve avere rapporti con o far parte del nucleo familiare degli amministratori esecutivi, dovendosi intendere per nucleo familiare quello costituito dal coniuge non separato legalmente, dai parenti ed affini entro il quarto grado;

(g) non deve avere relazioni di parentela, coniugio o affinità entro il quarto grado con componenti dell'organo di amministrazione, persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società, persone che esercitano, anche di fatto, la gestione e il controllo della Società e i sindaci della Società;

(h) deve avere e mantenere i requisiti di onorabilità indicati nel paragrafo 4.2.2.

4.2.2 Onorabilità e cause di ineleggibilità

Non può essere eletto Organismo di Vigilanza e, se lo è, decade necessariamente ed automaticamente dalla carica colui il quale:

(i) si trova nelle condizioni previste dall'articolo 2382 Codice civile, ovverosia gli inabilitati, interdetti, falliti o condannati ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;

(ii) sia stato sottoposto a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della Legge 27 dicembre 1956, n. 1423 (legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità) o della Legge 31 maggio 1965, n. 575 (legge contro la mafia);

(iii) sia stato condannato a seguito di sentenza ancorché non ancora definitiva, o emessa ex artt. 444 e ss. codice procedura penale o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

1) per uno dei delitti previsti nel Titolo XI del Libro V del Codice civile (Disposizioni penali in materia di società e consorzi) e nel Regio Decreto 16 marzo 1942, n. 267, e sue successive modifiche od integrazioni (Disciplina del fallimento, del concordato preventivo, dell'amministrazione controllata e della liquidazione coatta amministrativa);

2) per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;

3) alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;

4) in ogni caso e a prescindere dall'entità della pena per uno o più illeciti tra quelli tassativamente previsti dal D. Lgs. 231/01;

(iv) sia stato dichiarato interdetto, inabilitato o sottoposto a procedura fallimentare o essere stato condannato con sentenze che comportino l'interdizione dai pubblici uffici, dagli uffici direttivi delle imprese e delle persone giuridiche, da una professione o da un'arte e/o l'incapacità di contrattare con la Pubblica Amministrazione.

Analogamente, non può ricoprire il ruolo di Organismo di Vigilanza e, se lo è, decade necessariamente ed automaticamente dalla carica, colui nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* TUF (D. Lgs n. 58/1998) ovvero sia stata comminata una condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche.

4.2.3 Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale

L'Organismo di Vigilanza deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite alla sua indipendenza, ne garantiscono l'obiettività di giudizio; è necessario, pertanto, che l'Organismo di Vigilanza sia scelto tra soggetti in possesso di adeguate professionalità in materia di controllo e gestione dei rischi aziendali ed in materia giuridica.

L'Organismo di Vigilanza potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia giuridica di diritto penale, organizzazione aziendale, revisione, contabilità e finanza.

4.2.4 Continuità d'azione

L'Organismo di Vigilanza deve svolgere in modo continuativo le attività necessarie per la vigilanza in merito alla corretta applicazione del Modello con adeguato impegno e con i necessari poteri di indagine.

Adeguata informativa sul possesso dei requisiti sopra indicati sarà fornita al CdA al momento della nomina dell'OdV.

4.3 Durata in carica

Salvo diversa determinazione da parte del CdA, la durata dell'incarico dell'Organismo di Vigilanza è fissata in 3 (tre) anni, eventualmente rinnovabili con provvedimento del CdA.

Alla scadenza dell'incarico, l'OdV potrà continuare a svolgere le proprie funzioni e ad esercitare i poteri di propria competenza, come in seguito meglio specificati, sino alla nomina del nuovo OdV da parte del CdA.

L'Organismo di Vigilanza non può essere revocato se non per giusta causa, con delibera motivata della stessa. In tali casi, il CdA provvede alla nomina del nuovo OdV.

Rappresentano ipotesi di giusta causa di revoca:

(a) le violazioni al presente Modello;

(b) il verificarsi di una delle cause di incompatibilità di cui al precedente paragrafo 4.2;

(c) una sentenza di condanna della Società ai sensi del Decreto o una sentenza di patteggiamento, passata in giudicato, ove risulti dagli atti l'"omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;

(d) la mancata partecipazione a più di tre riunioni consecutive senza giustificazione;

(e) la negligenza nell'adempimento dei propri compiti;

(f) in caso di soggetti interni alla struttura aziendale, le eventuali dimissioni o licenziamento o comunque cessazione del rapporto di lavoro;

(g) il cambiamento dell'assetto azionario comportante la variazione del soggetto che dispone della maggioranza dei voti esercitabili nell'Assemblea ordinaria.

In caso di dimissioni o di decadenza automatica dell'Organismo di Vigilanza, quest'ultimo ne darà comunicazione tempestiva al CdA, che prenderà senza indugio le decisioni del caso.

È facoltà dell'OdV rinunciare in ogni momento all'incarico, dandone comunicazione scritta, motivando le ragioni della rinuncia, agli Organi Sociali. Tale rinuncia non ha effetto fino all'accettazione o alla nomina del nuovo OdV, e comunque non oltre 60 giorni dall'avvenuta comunicazione.

4.4 Funzione dell'Organismo di Vigilanza

All'OdV è affidato il compito di vigilare:

(a) sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;

(b) sull'osservanza del Modello da parte dei Destinatari;

(c) sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

Su di un piano più operativo all'OdV è affidato il compito di:

(i) *Aggiornamenti, potestà normativa, segnalazioni:*

a. interpretare la normativa rilevante e verificare l'adeguatezza del Modello a tali prescrizioni normative, segnalando al CdA le possibili aree di intervento;

b. verificare che gli elementi previsti dalla Parte Speciale del Modello per la prevenzione delle diverse tipologie di illeciti (adozione di clausole *standard*, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, proponendo, in caso contrario, un aggiornamento degli elementi stessi;

c. promuovere la revisione e l'eventuale aggiornamento del Modello in relazione a: (a) accertamento di violazioni delle prescrizioni del Modello, (b) rilevanti modificazioni dell'assetto interno della Società, delle attività d'impresa o delle relative modalità di svolgimento e/o (c) modifiche normative (ad esempio inserimento di nuovi reati- presupposto nel D. Lgs. 231/2001), segnalando al CdA le possibili aree di intervento;

d. promuovere, qualora risulti che lo stato di attuazione delle prescrizioni del Modello sia carente, tutte le iniziative necessarie al fine di far adeguare i comportamenti alle previsioni del Modello stesso;

e. coordinarsi con i responsabili delle altre Funzioni aziendali e/o di Gruppo per i diversi aspetti attinenti all'attuazione del Modello (definizione delle clausole standard, formazione, provvedimenti disciplinari, ecc.);

f. verificare periodicamente – con il supporto delle altre Funzioni competenti – il sistema di poteri in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti;

g. informare tempestivamente il CdA e i sindaci in relazione a eventuali gravi violazioni del Modello, richiedendo il supporto delle Funzioni in grado di collaborare nell'attività di verifica e di individuazione delle azioni idonee a impedire il ripetersi delle circostanze in questione.

(ii) *Verifiche e controlli:*

a. condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle Attività Sensibili;

b. in ottemperanza a quanto previsto nel calendario annuale delle attività dell'OdV, effettuare periodiche verifiche mirate su determinate operazioni o specifici atti posti in essere nell'ambito delle Attività Sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi in sede di *reporting* agli Organi Sociali deputati;

c. raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere ad esso trasmesse o tenute a propria disposizione;

d. coordinarsi con le Funzioni (anche attraverso apposite riunioni) per il miglior monitoraggio delle Attività Sensibili. A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale (sia cartacea sia informatica) che ritiene rilevante e deve essere costantemente informato dal *management*: a) sugli aspetti dell'attività aziendale che possono esporre la Società al rischio di commissione di uno dei Reati;
b) sui rapporti con Collaboratori, Consulenti, *Partner*, Fornitori e Terze Parti;

e. vigilare sull'attuazione delle procedure di controllo previste dal Modello;

f. verificare prontamente ogni criticità riscontrata dai competenti esponenti aziendali, proponendo le opportune soluzioni operative;

g. verificare che le azioni correttive necessarie per rendere il Modello adeguato ed efficace siano prontamente attuate.

(iii) *Formazione:*

a. promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello;

b. concorrere a definire i programmi di formazione e il contenuto delle comunicazioni periodiche da farsi agli Organi Sociali;

(iv) *Violazioni del Modello e Sanzioni:*

a. nel caso si ritenga necessario effettuare investigazioni interne, assumere un ruolo di coordinamento e supervisione in relazione a tali indagini, avvalendosi – per lo svolgimento delle attività investigative – di una Funzione aziendale e/o di Gruppo o di una combinazione di Funzioni e/o di consulenti esterni;

b. coordinarsi con il *management* aziendale per valutare o proporre l'adozione di eventuali sanzioni o provvedimenti per le violazioni del Modello, fermo restando la competenza di quest'ultimo - e in particolare degli incaricati della gestione delle risorse umane - in merito alla decisione e alla irrogazione dei medesimi (si rinvia in merito a questo punto al successivo Capitolo 6 della presente Parte Generale).

4.5 Poteri dell'Organismo di Vigilanza

L'OdV ha, *ex lege*, autonomi poteri di iniziativa e controllo ai fini di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento sulla struttura aziendale o sanzionatori, poteri questi che sono demandati ai competenti Organi Sociali o alle Funzioni competenti.

Tenuto conto delle peculiarità delle attribuzioni e degli specifici contenuti professionali richiesti, nello svolgimento dei compiti di vigilanza e controllo, l'OdV sarà comunque costantemente supportato anche dal *management* della Società.

In capo al *management*, nell'ambito delle rispettive funzioni e nei limiti dei poteri assegnati, ricade una responsabilità primaria per quanto concerne: 1) il controllo delle attività e delle aree di competenza; e 2) la tempestiva e puntuale informazione verso l'OdV su eventuali anomalie, problematiche riscontrate e/o criticità rilevate.

L'OdV potrà richiedere alle Funzioni competenti specifiche attività di controllo al fine del corretto e preciso funzionamento del Modello.

Tutti i soggetti coinvolti all'interno della Società sono tenuti a vigilare ed informare l'OdV sulla corretta applicazione del presente Modello, ciascuno nell'ambito delle proprie competenze operative.

L'OdV può avvalersi, ogni qualvolta lo ritiene necessario all'espletamento della propria attività di vigilanza e di tutto quanto previsto nel presente Modello, della collaborazione di ulteriori risorse di volta in volta ritenute necessarie, prescelte nell'ambito delle varie Funzioni, senza limitazioni di tempo e di numero, che potranno altresì costituire uno staff dedicato, a tempo pieno o *part-time*, qualora ne venisse ravvisata la necessità.

Peraltro, nei casi in cui si richiedano attività che necessitano di professionalità non presenti all'interno della Società, l'OdV potrà avvalersi di consulenti esterni.

Pertanto, all'OdV sono conferiti i seguenti poteri:

- potere di accedere a tutti i documenti e a tutte le informazioni relative alla Società;
- potere di avvalersi di tutte le Funzioni, che sono obbligate a collaborare, e di consulenti esterni;
- potere di raccogliere informazioni presso tutti i Destinatari del presente Modello, incluse le Terze Parti, in relazione a tutte le attività della Società;
- potere di richiedere, attraverso i canali e le persone appropriate, la convocazione del CdA e dei sindaci per affrontare questioni urgenti;
- potere di richiedere ai responsabili delle Funzione di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza;
- potere di avvalersi di consulenti esterni ai quali delegare circoscritti ambiti di indagine o attività. A tale proposito, il CdA dovrà approvare ogni anno un *budget* di spesa per l'OdV, il quale ne potrà disporre liberamente in relazione alle proprie attività, salvo richieste integrazioni per eventuali necessità sopravvenute.

4.6 Regole di convocazione e di funzionamento

L'Organismo di Vigilanza può disciplinare con specifico regolamento le modalità del proprio funzionamento, sulla base dei principi di seguito riportati:

- l'Organismo di Vigilanza redige verbali (almeno ogni sei mesi ovvero ad evento) sull'andamento delle attività di vigilanza;

- gli Organi Sociali possono richiedere che l'Organismo di Vigilanza sia convocato nelle riunioni del CdA o del Collegio Sindacale in qualsiasi momento;
- possono essere effettuate sedute *ad hoc* con le Funzioni e tutte le decisioni prese durante queste sedute devono essere tracciate in forma scritta;
- i verbali delle sedute riportano tutte le decisioni prese dall'Organismo di Vigilanza e riflettono le principali considerazioni effettuate per raggiungere la decisione; tali verbali vengono conservati dall'Organismo di Vigilanza nel proprio archivio.

4.7 Reportistica dell'Organismo di VigilanzaL'OdV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

Sono assegnate all'OdV due linee di reporting:

- la prima, su base continuativa, direttamente verso il Presidente del CdA;
- la seconda, su base periodica almeno annuale, nei confronti dell'intero CdA.

Tali flussi informativi hanno ad oggetto:

1) l'attività svolta dall'OdV;
2) le eventuali criticità (e spunti di miglioramento) emerse sia in termini di comportamenti o eventi interni, sia in termini di efficacia del Modello.

Nel proprio *reporting* annuale l'OdV trasmette al CdA una relazione scritta sull'attuazione del Modello che contiene:

(a) un'analisi sintetica di tutta l'attività svolta nel corso dell'anno (indicando in particolare i controlli e le verifiche specifiche effettuati e l'esito degli stessi, l'eventuale aggiornamento della mappatura delle Attività Sensibili, ecc.);

(b) un piano di attività prevista per l'anno successivo.

Gli incontri con gli organi cui l'OdV riferisce devono essere verbalizzati e copie dei verbali devono essere custodite dall'OdV.

Il Presidente del CdA ha facoltà di convocare in qualsiasi momento l'OdV che, a sua volta, ha la facoltà di richiedere, attraverso le Funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

4.8 Flussi informativi nei confronti dell'Organismo di Vigilanza

L'OdV esercita le proprie responsabilità di verifica e controllo anche attraverso l'analisi di sistematici flussi informativi.

Le suddette informazioni e la documentazione da trasmettere e/o da mettere a disposizione dell'OdV, con le relative tempistiche ed i canali informativi da utilizzare, sono individuate nella Parte Speciale del Modello.

I flussi comunicativi verso l'OdV, si dividono in:

a. Flussi ad evento; e

b. Flussi periodici.

I flussi informativi di cui sopra devono essere trasmessi dalle competenti Funzioni alla casella di posta elettronica dell'OdV: Unikeris.odv@unikeris.com.

Flussi informativi ad evento

I flussi ad evento devono essere trasmessi in forma scritta (mediante la casella postale dell'OdV: Unikeris.odv@unikeris.com), ovvero in ogni altra modalità ritenuta comunque idonea da parte dell'OdV, a seguito del verificarsi di determinati eventi, caratterizzati da anomalia o atipicità, attinenti all'attuazione del Modello e delle procedure aziendali ivi richiamate in relazione alle Attività Sensibili, che possano essere ritenute utili ai fini dell'assolvimento dei compiti dell'Organismo di Vigilanza.

In particolare, a titolo indicativo e non esaustivo, si sottolinea l'importanza delle seguenti comunicazioni:

1. ogni rilevante emanazione, modifica e/o integrazione del sistema organizzativo aziendale della Società e/o dell'assetto societario (operazioni straordinarie, ecc.), quali modifiche e variazioni al sistema delle deleghe e procure conferite, all'organigramma, ecc.;

2. richieste di assistenza legale inoltrate dagli Organi Sociali nei confronti dei quali la magistratura proceda per i reati di cui al Decreto;

3. qualsiasi intervento di natura ispettiva da parte di organismi pubblici (magistratura, Guardia di Finanza, altre Autorità, ecc.) oppure enti terzi privati (*i.e.* enti di certificazione, audit da parte di soggetti esterni alla Società);

4. esiti delle verifiche ispettive condotte da Autorità esterne (*i.e.* AdE, GdF, Isp. Lav, C.C. ecc.), dai quali emergono significativi rilievi, raccomandazioni e/o eventuali sanzioni dalle stesse applicate alla Società;

5. provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini o procedimenti, anche nei confronti di ignoti, per i reati ex D. Lgs. 231/2001 qualora tali indagini coinvolgano la Società o suoi esponenti, Organi Sociali, le Funzioni che svolgono attività a favore della Società, Collaboratori, Consulenti, *Partner*, e Fornitori;

6. esiti dei controlli di primo livello, dei controlli effettuati per dare attuazione al Modello e delle attività di investigazione interna dai quali risultino criticità/anomalie significative dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità/responsabilità rispetto all'osservanza delle previsioni del Modello e alla corretta attuazione dello stesso;

7. eventuali comunicazioni da parte del Collegio Sindacale in merito ad anomalie/criticità riscontrate nello svolgimento dell'attività di valutazione e controllo sull'adeguatezza dell'assetto organizzativo e del sistema di controllo interno della Società;

9. operazioni finanziarie/societarie significative o atipiche che possano essere a rischio reato;

10. i procedimenti sanzionatori svolti e le eventuali sanzioni irrogate ovvero i provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello.

Ad integrazione dei flussi informativi ad evento di cui sopra, si rinvia alla Parte Speciale del Modello per l'individuazione delle ulteriori circostanze che determinano l'obbligo di invio di flussi comunicativi ad evento all'OdV.

L'OdV può comunque richiedere, in piena autonomia, ulteriori informazioni di carattere periodico ovvero notizie concernenti specifiche situazioni a qualunque Funzione o struttura aziendale. Deve essere cura delle Funzioni provvedere a mantenere a disposizione tutta la documentazione relativa alle informative trasmesse all'OdV.

Qualora uno dei soggetti tenuti alla trasmissione dei flussi informativi periodici non adempia agli obblighi informativi di cui al presente paragrafo, allo stesso sarà irrogata una sanzione disciplinare che varierà a seconda della gravità dell'inottemperanza agli obblighi sopra menzionati e che sarà proposta dall'OdV e comminata secondo le regole indicate nel presente Modello.

Flussi informativi con cadenza periodica

Oltre alle informazioni di carattere tempestivo di cui sopra, devono essere trasmesse all'OdV, da parte delle Funzioni competenti, incluse le Funzioni esternalizzate ad altre società del Gruppo o a Terze Parti (così come individuate nella Parte Speciale), tutte le informazioni utili a garantire all'OdV un'efficace informazione ai fini delle attività di vigilanza.

Sulla base della periodicità definita nella Parte Speciale, il responsabile indicato della rispettiva Funzione provvede a fornire le informazioni riportate attraverso comunicazione via mail alla casella di posta elettronica dell'OdV (Unikeris.odv@unikeris.com).

Si rinvia alla Parte Speciale del Modello per l'esatta individuazione delle circostanze che determinano l'obbligo di invio dei flussi comunicativi periodici (a cadenza trimestrale, semestrale, annuale) all'OdV.

4.9 Segnalazioni di condotte rilevanti ai fini del Modello

Oltre al sopra delineato sistema di flussi informativi, che assume valore tassativo, chiunque venga a conoscenza, in ragione delle mansioni svolte, di condotte illecite rilevanti ai sensi del Decreto o di qualsiasi violazione del presente Modello è tenuto a darne immediata notizia mediante *SpeakUp&BeHeard*. In caso di segnalazioni che si rivelino infondate, effettuate con dolo o colpa grave, verranno applicate le misure di cui al Sistema Disciplinare.

SpeakUp&BeHeard è il sistema di comunicazione e gestione delle segnalazioni adottato dal Gruppo Chiesi. Tale sistema, composto da una piattaforma *web* (che non risiede nel sistema informatico del Gruppo, in quanto ospitata su un *server* indipendente) e da una casella vocale, è accessibile da chiunque intenda effettuare una segnalazione e prevede la possibilità per il segnalante che preferisca effettuare la segnalazione in forma orale di richiedere un incontro diretto con la Società.

Il sistema è strutturato in modo da garantire (anche con modalità informatiche) i più elevati livelli di confidenzialità con riferimento alla segnalazione, all'identità del segnalante e della persona oggetto della segnalazione (salvi gli obblighi di legge e la tutela dei diritti della Società e delle persone accusate erroneamente e/o in mala fede), nonché la riservatezza, sicurezza, non tracciabilità e integrità dei dati relativi alla segnalazione, conformemente a quanto previsto dal Decreto 24/23.

In caso di segnalazioni effettuate con modalità differenti, la Società non potrebbe garantire i medesimi livelli di protezione. In particolare, qualora la segnalazione venisse effettuata tramite posta elettronica, l'anonimato potrebbe non essere garantito.

Le segnalazioni afferenti a Unikeris trasmesse attraverso *SpeakUp&BeHeard* saranno gestite dall'OdV di Unikeris, dotato dei requisiti previsti dal Decreto 24/23 per l'organo deputato alla gestione delle segnalazioni.

In ogni caso, la Società verifica e assicura che i segnalanti non siano soggetti ad alcuna forma di ritorsione, discriminazione o penalizzazione, diretta o indiretta, per motivi collegati, direttamente o indirettamente, alla segnalazione. In particolare, nessuno può essere sottoposto ad alcuna delle azioni ritorsive previste dall'art. 17 del Decreto 24/23 (a titolo esemplificativo: coercizione, intimidazione, discriminazione o comunque trattamenti sfavorevoli, conclusione anticipata o annullamento del contratto di fornitura di beni o servizi), fermo restando l'applicazione delle misure previste nel Sistema Disciplinare nei confronti di chi effettua segnalazioni (rivelatesi infondate) con dolo o colpa grave.

Il processo di trasmissione e gestione delle segnalazioni, nonché i ruoli e le responsabilità dei soggetti coinvolti nel processo sono definiti all'interno delle *Guideline* e della SOP "Utilizzo e gestione di *SpeakUp&BeHeard*".

4.10 Obblighi di riservatezza

L'OdV adempie al proprio incarico con la diligenza richiesta dalla natura dell'incarico e dell'attività esercitata nonché dalle sue specifiche competenze.

L'OdV è tenuto al rispetto degli obblighi di riservatezza in ordine alle notizie ed informazioni acquisite nell'esercizio delle proprie funzioni.

4.11 Raccolta e conservazione delle informazioni

Ogni informazione raccolta e ogni *report* ricevuto o preparato dall'Organismo di Vigilanza è conservato per 10 anni in un apposito archivio tenuto dall'OdV in formato cartaceo o elettronico.

CAPITOLO 5: LA DIFFUSIONE E LA FORMAZIONE

5.1 La diffusione

In linea con quanto disposto dal D.Lgs. 231/2001 e dalle Linee Guida di Confindustria, la Società dà piena pubblicità al presente Modello, mediante i canali di comunicazione più appropriati.

La comunicazione deve essere capillare, efficace, chiara e dettagliata, con aggiornamenti periodici connessi ai mutamenti del Modello, in osservanza di quanto previsto dalle Linee Guida di Confindustria.

L'adozione del presente Modello e i successivi aggiornamenti sono comunicati a (i) tutti i componenti degli Organi Sociali, (ii) alle Funzioni e (iii) alle Terze Parti.

In caso di dimissioni e/o revoca dei componenti degli Organi Sociali e in caso di nuove assunzioni all'interno delle Funzioni di Gruppo, ai nuovi componenti viene consegnato un *set* informativo con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza connesse al Modello 231.

5.2 La formazione

La formazione è circoscritta ai soli Organi Sociali e – laddove se ne ravvisi la necessità – alle Funzioni di Gruppo e/o Terze Parti.

La formazione, gestita dalla Società con la supervisione dell'OdV, si pone come obiettivo quello di far conoscere il Modello adottato dalla Società e di sostenere adeguatamente tutti coloro che sono coinvolti nell'espletamento delle Attività Sensibili.

A tale riguardo periodicamente sarà predisposto, con la collaborazione dell'OdV, un piano di formazione che tenga in considerazione, in particolare, le specifiche esigenze emerse in relazione alla peculiare operatività aziendale di riferimento.

La formazione deve essere caratterizzata da capillarità, efficacia, autorevolezza e chiarezza e deve essere adeguatamente dettagliata nonché periodicamente ripetuta, ad intervalli regolari.

In particolare, la Società cura l'adozione e l'attuazione di un adeguato livello di formazione mediante idonei strumenti di diffusione, inclusa l'organizzazione di *meeting* aziendali.

I contenuti formativi sono aggiornati in relazione all'evoluzione della normativa e del Modello: pertanto qualora intervengano modifiche rilevanti (es. estensione della responsabilità amministrativa della Società a nuove tipologie di reati), si procede ad una coerente integrazione dei contenuti medesimi, assicurandone altresì la fruizione.

La mancata partecipazione all'attività di formazione senza giustificazione da parte dei componenti degli Organi Sociali e/o delle Funzioni di Gruppo costituisce una violazione dei principi contenuti nel presente Modello e, pertanto, sarà sanzionata ai sensi di quanto indicato nel capitolo 6 che segue.

L'Organismo di Vigilanza verifica periodicamente lo stato di attuazione del piano di formazione.

CAPITOLO 6: IL SISTEMA DISCIPLINARE

6.1 Funzione del Sistema Disciplinare

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di adeguata efficacia deterrente) applicabili in caso di violazione delle regole di cui al presente Modello, rende effettiva l'azione di vigilanza dell'OdV ed ha lo scopo di garantirne l'efficace attuazione.

La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'art. 6, comma 1, lett. *e)*, D.Lgs. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità della Società.

L'applicazione del sistema sanzionatorio e dei relativi provvedimenti è indipendente dallo svolgimento e dall'esito del procedimento penale che l'autorità giudiziaria abbia eventualmente avviato nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001, in quanto le regole di condotta imposte dal Modello sono assunte dalla Società in piena autonomia, indipendentemente dall'illecito che eventuali comportamenti possano determinare.

Inoltre, il presente Sistema Disciplinare deve essere adeguatamente diffuso in quanto parte integrante dell'attuazione del Modello, attraverso un'adeguata attività di informazione e formazione.

Il presente capitolo contiene la descrizione delle misure sanzionatorie adottate dalla Società in caso di violazione del Modello da parte dei Destinatari.

6.2 Le condotte rilevanti

Ai fini del presente Sistema Disciplinare, costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del Modello 231 adottato dalla Società.

Sono sanzionabili, a mero titolo esemplificativo e non esaustivo, i seguenti comportamenti:

1. mancato rispetto del Modello, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto, o comunque sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto;
2. mancato rispetto del Modello, qualora si tratti di violazione idonea ad integrare il solo fatto (elemento oggettivo) di uno dei reati previsti nel Decreto;
3. mancato rispetto del Modello, qualora si tratti di violazioni connesse, in qualsiasi modo, alle aree "a rischio reato" o alle Attività Sensibili;
4. le violazioni di procedure interne richiamate nel presente Modello;

5. mancata collaborazione, quando richiesta, con l'Organismo di Vigilanza;

6. omesso invio di flussi informativi/segnalazioni ai sensi del Modello, quando ripetuto e diretto a ostacolare le funzioni dell'Organismo di Vigilanza;

7. ripetuta mancata partecipazione, non adeguatamente motivata, alla formazione relativa al Modello.

Inoltre, sono sanzionabili disciplinarmente:

(a) le condotte di chi pone in essere con dolo o colpa grave segnalazioni che si rivelano infondate;

(b) chi (i) adotta comportamenti ritorsivi, di cui all'art. 17 del Decreto 24/23, nei confronti del segnalante (e/o degli ulteriori soggetti di cui all'art. 3, comma 5, del Decreto 24/23) per motivi collegati, direttamente o indirettamente, alla segnalazione; (ii) viola le misure di tutela del segnalante, delle persone coinvolte e delle persone menzionate nella segnalazione di cui all'art. 12 del Decreto 24/23; oppure (iii) ostacola o ha tentato di ostacolare la segnalazione;

(c) i soggetti segnalati che siano ritenuti responsabili dei fatti oggetto della segnalazione.

Il sistema sanzionatorio è soggetto a costante verifica e valutazione da parte dell'Organismo di Vigilanza e del CdA, rimanendo quest'ultimo responsabile della concreta applicazione delle misure disciplinari sotto delineate su eventuale proposta dell'Organismo di Vigilanza.

Nell'ipotesi in cui la condotta in questione possa integrare una fattispecie di reato rilevante ai sensi del D. Lgs. 231/2001, l'attivazione del Sistema Disciplinare avviene indipendentemente dallo svolgimento e dall'esito dell'eventuale relativo procedimento penale.

6.3 Le sanzioni

L'individuazione e l'irrogazione delle sanzioni deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata.

A tale proposito, la gravità dell'infrazione sarà valutata sulla base delle seguenti circostanze:

- i tempi e le modalità concrete di realizzazione dell'infrazione;

- la presenza e l'intensità dell'elemento intenzionale;

- il livello di responsabilità e autonomia del soggetto autore dell'illecito disciplinare;
- l'entità del danno o del pericolo come conseguenza dell'infrazione per la Società;

- le circostanze nelle quali l'infrazione ha avuto luogo.

La recidiva costituisce un'aggravante ed implica l'applicazione di una sanzione più grave.

L'applicazione delle sanzioni di seguito indicate non pregiudica in ogni caso il diritto della Società di agire nei confronti del soggetto responsabile al fine di ottenere il risarcimento di tutti i danni patiti a causa o in conseguenza della condotta accertata.

6.4 Misure nei confronti degli amministratori e dei procuratori

Qualora sia riscontrata la violazione del Modello da parte di un amministratore o di un procuratore, l'OdV trasmette al Consiglio di Amministrazione ed al Collegio Sindacale una relazione contenente gli estremi della condotta, i riscontri documentali nonché un'eventuale proposta in merito alla sanzione opportuna.

Il Consiglio di Amministrazione può effettuare ulteriori accertamenti e, sulla scorta dei relativi esiti, provvederà a determinare la sanzione ritenuta applicabile, motivando l'eventuale dissenso rispetto alla proposta formulata dall'OdV.

In particolare, potranno essere applicate le seguenti sanzioni:

- il richiamo scritto;
- la diffida al puntuale rispetto delle previsioni del Modello;
- la revoca dall'incarico.

6.5 Misure nei confronti dei Sindaci

L'Organismo di Vigilanza, qualora riscontri la violazione del Modello da parte di un membro del Collegio Sindacale, trasmette al Consiglio di Amministrazione e al Collegio Sindacale una relazione contenente gli estremi della condotta, i riscontri documentali nonché un'eventuale proposta in merito alla sanzione opportuna.

Il Consiglio di Amministrazione può effettuare ulteriori accertamenti e, sulla scorta dei relativi esiti, provvederà a determinare la sanzione ritenuta applicabile, motivando l'eventuale dissenso rispetto alla proposta formulata dall'OdV.

In particolare, potranno essere applicate le seguenti sanzioni:

- la diffida al puntuale rispetto delle previsioni del Modello; ovvero

- la revoca dell'incarico.

6.6 Misure nei confronti di Terze Parti

Qualora riscontri la violazione del Modello da parte di Terze Parti, l'OdV trasmette alla Funzione preposta alla gestione del rapporto contrattuale in questione una relazione contenente gli estremi della condotta, i riscontri documentali nonché un'eventuale proposta in merito alla sanzione opportuna.

La Funzione interessata si pronuncia in ordine alla determinazione ed alla concreta applicazione della misura, motivando l'eventuale dissenso rispetto alla proposta formulata dall'OdV.

La Funzione invia, quindi, alle Terze Parti una comunicazione scritta, contenente l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione nonché il rimedio contrattualmente previsto applicabile. La Funzione interessata provvede anche all'effettiva applicazione della sanzione nel rispetto delle norme di legge e di regolamento applicabili.

L'OdV, cui è inviata per conoscenza la comunicazione, verifica l'applicazione del rimedio contrattuale applicabile.

CAPITOLO 7: LE VERIFICHE SULL'ADEGUATEZZA DEL MODELLO

L'effettiva applicazione del Modello e la sua efficace attuazione devono essere oggetto di adeguate attività di controllo.

Queste attività sono svolte in primo luogo dalle Funzioni competenti.

In aggiunta, anche l'OdV – oltre all'attività di vigilanza svolte continuativamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei Destinatari ed il Modello stesso) – effettua periodicamente specifiche verifiche sulla idoneità del Modello a prevenire la commissione dei Reati e sulla sua conformità alla normativa in materia di responsabilità amministrativa degli enti, nell'ambito del periodico aggiornamento del Modello medesimo.

Infine, viene svolta dall'OdV una *review* di tutte le segnalazioni ricevute nel corso dell'anno e degli eventi considerati rischiosi, delle azioni intraprese dall'OdV e della consapevolezza degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa con verifiche a campione.

Per le verifiche l'OdV si avvale, di norma, del supporto dei responsabili delle Funzioni competenti e, ove necessario, di consulenti esterni.

Le verifiche e il loro esito sono oggetto di *report* annuale al CdA. In particolare, in caso di esito negativo, l'OdV esporrà, nel piano relativo all'anno, i miglioramenti da attuare.

CAPITOLO 8: LE COMPONENTI DEL MODELLO

8.1 Gli elementi del Modello

Il presente Modello 231 è strutturato su tre livelli: (1) organizzazione, (2) presidi generali di controllo e (3) protocolli di controllo specifici.

8.2 Elementi organizzativi del Modello

Le componenti organizzative del Modello 231 della Società sono costituite da:

- **Norme interne**: le regole contenute in questo Modello, ivi inclusi le regole di comportamento, i divieti e i presidi di controllo presenti nella Parte Speciale del Modello, così come le regole di condotta specifiche, le politiche e procedure adottate dalla Società in attuazione del Modello;
- **Struttura organizzativa:** la presenza di una organizzazione aziendale coerente con le attività aziendali, idonea ad assicurare la correttezza dei comportamenti, nonché a

garantire una chiara ed organica attribuzione dei compiti ed una appropriata segregazione delle funzioni, assicurando che gli assetti previsti dalla struttura organizzativa siano realmente attuati e oggetto di controllo, attraverso: (i) contratti di servizi con società del Gruppo o soggetti terzi, ai quali sono esternalizzate specifiche attività aziendali; (ii) un'architettura di poteri (deleghe e procure) formalizzata, che costituisce parte integrante e sostanziale del Modello;

- **Organismo di Vigilanza**: è l'organismo creato in virtù del Modello, dotato di autonomia, indipendenza, continuità di azione e professionalità, che ha il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporne l'aggiornamento; è dotato di capacità di spesa, supporto delle Funzioni e di potere di accesso alle informazioni aziendali.

8.3 I presidi generali di controllo

Di seguito sono indicati i presidi generali che sono previsti come parte essenziale del Modello e devono essere sempre applicati e rispettati con riferimento a tutte le Attività Sensibili prese in considerazione dalla Parte Speciale del Modello 231:

8.3.1 Il Codice di Condotta

L'adozione di principi etici rilevanti ai fini della prevenzione dei reati di cui al D. Lgs. 231/2001 rappresenta un obiettivo del presente Modello.

In tale ottica, l'adozione di un Codice di Condotta quale utile strumento di governance costituisce un elemento essenziale del sistema di controllo preventivo. Il Codice di Condotta, infatti, mira a raccomandare, promuovere o vietare determinati comportamenti a cui possono essere collegate sanzioni proporzionate alla gravità delle eventuali infrazioni commesse.

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice di Condotta, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice di Condotta.

Il Codice di Condotta esprime i principi di "deontologia aziendale" che Chiesi riconosce come propri e sui quali richiama l'osservanza da parte di tutto il Gruppo. Esso assolve ad una duplice funzione: da un lato, definisce i valori e i principi etici cui il Gruppo si ispira nell'espletamento della missione aziendale; dall'altro, individua specifiche norme comportamentali, cui tutti i soggetti destinatari del Codice di Condotta devono attenersi.

8.3.2 La *Policy Anti-Bribery*

In data 5 dicembre 2022 il CdA di UNIKERIS ha approvato la *Policy Anti-Bribery* di Chiesi. La *Policy* è un documento di Gruppo che fissa un *set* di regole comuni in materia di anticorruzione applicabili a tutti gli *stakeholder* (sia interni che esterni) del Gruppo.

8.3.3 Sistema dei poteri

La Società adotta e mantiene aggiornato nel tempo un sistema di poteri basato su deleghe di poteri, procure e protocolli di approvazione dei costi interni e dell'operatività dei conti bancari.

I poteri sono strettamente connessi e coerenti alle responsabilità organizzative e gestionali assegnate e circoscritti a specifici limiti di valore.

L'attribuzione di poteri risponde ai seguenti principi inderogabili:

- definizione di ruoli, responsabilità e controlli nel processo di conferimento;
- conferimento, aggiornamento e revoca di poteri in coerenza con i ruoli ricoperti nell'organizzazione, con allineamento in caso di cambiamenti dell'organizzazione o di variazione di ruoli e responsabilità individuali o di uscita/ingresso di persone;
- tempestiva e costante diffusione delle informazioni circa la titolarità dei poteri attribuiti ed i relativi cambiamenti;
- tracciabilità e archiviazione di tutta la documentazione relativa ai poteri conferiti e relative variazioni;
- verifica periodica della conformità dell'esercizio dei poteri di rappresentanza con le procure conferite;
- monitoraggio periodico dell'adeguatezza del sistema dei poteri e relativo aggiornamento, avuto riguardo alla eventuale evoluzione dell'attività della Società.

8.3.4 Segregazione

Lo svolgimento delle Attività Sensibili deve fondarsi sul principio della segregazione delle funzioni: il soggetto che assume la decisione e che la attua deve essere diverso per quanto possibile dal soggetto incaricato di effettuare i controlli. La separazione dei compiti deve essere assicurata dall'intervento di più soggetti all'interno di un medesimo processo e può essere attuata tramite l'utilizzo di sistemi informatici che permettono soltanto a specifiche

persone identificate e autorizzate di effettuare determinate operazioni. Ove la separazione dei compiti non possa essere pienamente garantita sono previsti controlli compensativi.

Questo presidio si pone come obiettivo quello di evitare che un soggetto si trovi nella situazione di poter nascondere errori od irregolarità, relativi ad un'operazione commessa nello svolgimento delle proprie mansioni, senza che altri colleghi impegnati nella stessa operazione riscontrino l'errore o l'irregolarità, con la fondamentale conseguenza che un'irregolarità potrebbe avvenire solamente in caso di collusione tra due o più responsabili.

8.3.5 Tracciabilità e archiviazione

Tutte le Attività Sensibili devono essere organizzate in modo da assicurare la tracciabilità documentale e la verificabilità *ex post* di ciascun passaggio rilevante del processo, nonché la corretta e documentata archiviazione e conservazione della documentazione rilevante in relazione a ciascun processo, per mezzo di supporti informatici e/o cartacei.

Questo presidio mira ad assicurare che tutte le operazioni aziendali siano autorizzate ad un predefinito livello e che siano supportate da adeguata documentazione, tale da assicurare la trasparenza delle operazioni stesse e da facilitarne in ogni momento la verifica.

8.3.6 Sistema di gestione dei processi esternalizzati

I processi esternalizzati ad altre società del Gruppo o a Terze Parti sono puntualmente identificati nella Parte Speciale del Modello.

Il ricorso all'esternalizzazione di funzioni comporta rilevanti benefici per la Società che, viste le sue ridotte dimensioni non potrebbe altrimenti dotarsi di una struttura interna in grado di gestire adeguatamente tutti i processi. Nel contempo, però, il Modello impone che le attività esternalizzate siano adeguatamente regolamentate da contratti i quali – a seconda dei casi – devono prevedere:

- che le attività esternalizzate, le modalità di esecuzione e il relativo corrispettivo siano adeguatamente definiti;
- che il fornitore si impegni ad una corretta esecuzione alle attività esternalizzate nel rispetto della normativa vigente e applicabile e delle disposizioni della Società;
- che il fornitore sia in possesso di tutte le autorizzazioni necessarie per svolgere l'incarico;
- che il fornitore garantisca – per quanto possibile - la continuità del servizio, la sicurezza e la riservatezza dei dati relativi alla Società; che le Funzioni della Società

abbiano – per quanto possibile - accesso e facoltà di controllo relativamente all'attività e alla documentazione del fornitore;

- che il contratto preveda adeguati rimedi a tutela della Società in caso di inadempienze contrattuali;

- che il fornitore si impegni a garantire lo svolgimento di tutte le attività nel rispetto delle leggi applicabili e delle policy di Gruppo (come previsto nel paragrafo 8.3.8).

8.3.7 Sistema di gestione e controllo dei flussi finanziari

La gestione finanziaria è supportata da processi autorizzativi delle spese strutturati e da strumenti informatici dedicati, impostati su *workflow* coerenti con i poteri di spesa e i ruoli organizzativi formalmente definiti.

Tali sistemi e processi sono ispirati ai principi di:

- separazione dei compiti (il soggetto richiedente la spesa è diverso dal soggetto che l'autorizza che è diverso da chi materialmente effettua il pagamento e lo registra);
- tracciabilità di tutti i movimenti finanziari e riconciliabilità degli stessi con il sistema amministrativo-contabile;
- individuazione del razionale della spesa da sostenere;
- previsione di forme di pagamento standard.

8.3.8 Controlli e monitoraggio

Il Modello prevede lo svolgimento di attività di verifica (periodica o *ad hoc*) in relazione a ciascuna Attività Sensibile e il monitoraggio delle Attività Sensibili in conformità a quanto previsto nel Modello.

8.3.9 Flussi informativi

Il Modello richiede che il soggetto responsabile dell'Attività Sensibile/processo di volta in volta considerato comunichi all'Organismo eventuali informazioni rilevanti in relazione alla specifica attività/processo, e in particolare la eventuale conoscenza di situazioni in cui l'Attività Sensibile/processo sia stata eseguita in violazione delle linee guida o procedure aziendali in vigore; richiede inoltre la predisposizione e l'aggiornamento di *report* periodici riepilogativi contenenti informazioni rilevanti in relazione all'Attività Sensibile/processo di volta in volta rilevanti.

8.3.10 Clausole contrattuali

All'interno dei contratti che regolano lo svolgimento delle Attività Sensibili devono essere inserite apposite clausole volte a tutelare la Società dalle condotte poste in essere dalle proprie controparti contrattuali, in violazione del Modello e delle procedure aziendali che di esso sono attuazione. Tali clausole prevedono ad esempio, ove applicabile: i) la dichiarazione da parte della controparte di conoscere e di impegnarsi a rispettare i principi della *Policy Anti- Bribery* e del Codice di Interdipendenza dei Fornitori adottati dal Gruppo; ii) la facoltà in capo alla Società di risolvere i contratti in questione in caso di violazione di tali obblighi; iii) il riferimento ad eventuali altre clausole rilevanti ai sensi del Modello, laddove rilevanti.

8.4 Protocolli di controllo della Parte Speciale

In aggiunta ai presidi generali sopra descritti e a quelli già adottati dalla Società, è prevista l'adozione di specifici protocolli di controllo che definiscano regole di comportamento, divieti e presidi di controllo associati alle Attività Sensibili della Società.

I Protocolli di Controllo formano la Parte Speciale del Modello 231.

UNIKERIS

Modello di organizzazione, gestione e controllo

ex D. Lgs. 231/2001

PARTE SPECIALE

N° VERSIONE	DATA	NOTE
01	31 maggio 2023	Prima emissione
02	luglio 2023	Seconda emissione
03	12 aprile 2024	Terza emissione
04	giugno 2026	Quarta emissione

Indice

1. PREMESSA 3

2. PRINCIPI DI COMPORTAMENTO GENERALI 6

3. PROCESSI SENSIBILI 231 8

3.1 *Regulatory* e Farmacovigilanza 8

3.2 Gestione delle attività di commercializzazione/fornitura del Prodotto 12

3.3 Gestione degli affari legali e societari 19

3.4 *Intellectual Property* 25

3.5 *Information Technology* 29

3.6 Finanza e fiscalità 34

3.7 Acquisti non core 40

4. FLUSSI INFORMATIVI 46

Allegati:

A. *Risk Assessment* – Mappatura Processi – Funzioni – Reati – Controlli

1. PREMESSA

Unikeris ha svolto - preliminarmente all'adozione del presente Modello - un'attività di *risk assessment* finalizzata all'individuazione delle Attività Sensibili, ossia delle attività esposte al rischio di commissione di Reati Presupposto ai sensi del D.Lgs. 231/2001. A fronte dell'individuazione delle Attività Sensibili relative a ciascun processo aziendale sono stati poi predisposti i rispettivi Protocolli di Controllo riflessi nella presente Parte Speciale, ossia le regole di comportamento, i divieti e i controlli finalizzati a prevenire, con riferimento a ciascun processo aziendale, la commissione dei Reati Presupposto.

Ai fini dello svolgimento del *risk assessment* sono state organizzate sessioni di *workshop* con i soggetti responsabili dello svolgimento delle attività aziendali, nel corso dei quali è stata illustrata la finalità del *risk assessment* e sono state ripercorse sinteticamente le caratteristiche e le modalità di svolgimento di ciascuna Attività Sensibile in relazione agli scenari di rischio reato rilevanti, al fine di individuare i presidi di controllo già implementati ed adottati dalla Società nell'ambito dello svolgimento delle Attività Sensibili e di valutare i rischi 231 insiti in ciascuna attività.

L'Allegato "*Risk Assessment – Mappatura Processi – Funzioni – Reati – Controlli*" contiene per ciascun Processo:

- Reati Presupposto ai quali la Società è potenzialmente esposta in relazione a ciascun Processo; a questo proposito si segnala che l'esposizione al rischio può essere "diretta", nei casi in cui l'attività aziendale sia condotta in un modo improprio al fine di commettere il Reato, ma anche "indiretta" o "strumentale", allorché l'attività sia condotta in modo improprio al fine di agevolare od occultare la commissione di un Reato nell'ambito di altra attività aziendale;
- Possibili modalità di realizzazione delle condotte dei reati a rischio;
- Soggetti coinvolti in ciascuna Attività Sensibile, con particolare riferimento a Funzioni aziendali e/o di Gruppo, nonché Terze Parti, Collaboratori, Consulenti, *Partner*, Fornitori ed eventuali P.A. / Pubblici Ufficiali coinvolti;
- Controlli orizzontali, ossia i presidi generali che sono previsti come parte essenziale del Modello e devono essere sempre applicati e rispettati con riferimento a tutte le Attività Sensibili prese in considerazione dalla presente Parte Speciale del Modello 231 (es. separazione dei compiti, tracciabilità e archiviazione, sistema dei poteri, etc.);

- Controlli verticali, ossia i presidi di controllo specifici, anche procedurali, adottati dalla Società in relazione a ciascuna Attività Sensibile.

Si evidenzia che all'esito delle attività di *risk assessment* effettuate il rischio di commissione di Reati Presupposto si considera, nel complesso, limitato. Il disegno della presente Parte Speciale è stato pertanto improntato ad un criterio di proporzionalità, in ragione del quale le regole e controlli stabiliti sono proporzionati alle ridotte dimensioni e alla struttura della Società.

La presente Parte Speciale indica i Processi che caratterizzano l'operatività della Società, le relative Attività Sensibili, svolte dalla Società sia direttamente sia tramite altre società del Gruppo e/o Terze Parti, e i rispettivi Protocolli di Controllo. Per ciascun Processo sono indicati:

a. **Attività Sensibili**: descrizione delle Attività Sensibili relative a ciascun Processo;
b. **Reati Presupposto**: indicazione delle famiglie di Reato rilevanti per le Attività Sensibili;
c. **Regole di comportamento**: le regole di condotta che i principali soggetti coinvolti nel Processo devono rispettare;
d. **Divieti**: i divieti che i principali soggetti coinvolti nel Processo devono rispettare;
e. **Controlli specifici**: i controlli che le funzioni aziendali competenti devono attuare nello svolgimento delle proprie attività;
f. **Controlli procedurali**: le procedure aziendali disciplinanti le Attività Sensibili oggetto della presente Parte Speciale.

In particolare, sono stati individuati e valorizzati specifici "snodi di processo" che prevedono controlli non aggirabili anche in caso di "violazione frontale" delle regole, al fine di rendere più efficace l'applicazione, il monitoraggio e l'audit del Modello (i "**Punti di Controllo**").

La metodologia sopra descritta verrà adottata anche in occasione di ogni successivo aggiornamento del Modello, qualora gli interventi abbiano carattere sostanziale e comportino pertanto l'individuazione di nuove Attività Sensibili, la valutazione di nuovi Reati Presupposto o l'introduzione di nuovi Punti di Controllo.

La presente Parte Speciale costituisce parte integrante del Modello di Unikeris e si applica – per quanto di rispettiva rilevanza - a tutti i Destinatari del Modello che si trovano coinvolti nello svolgimento delle Attività Sensibili, ivi inclusi:

- le persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società;
- i Partner, Fornitori, Collaboratori, Consulenti e in generale le Terze Parti che operano in nome o per conto o comunque nell'interesse della Società, sotto la vigilanza dei soggetti apicali.

L'eventuale inosservanza della presente Parte Speciale comporta l'applicazione di sanzioni disciplinari, in conformità con quanto previsto dalla legge, dalle norme contrattuali vigenti e dal sistema disciplinare adottato dalla Società (v. Parte Generale del Modello 231).

Tutti i termini indicati con lettera maiuscola nella presente Parte Speciale hanno il medesimo significato agli stessi attribuito nella Parte Generale del Modello 231 della Società.

Ai fini della presente Parte Speciale rilevano inoltre le seguenti definizioni, ulteriori rispetto a quelle indicate nella Parte Generale:

- "Destinatari": i soggetti indentificati nel paragrafo "Destinatari del Modello" della Parte Generale.
- "Procedure aziendali": *policies*, *guidelines*, istruzioni operative, sop aziendali e/o di Gruppo rilevanti nello svolgimento delle Attività Sensibili;
- "Processi": macroaree di attività in cui è organizzata l'operatività della Società; e
- "Protocolli di Controllo": le regole di comportamento, i divieti e i controlli finalizzati a prevenire, con riferimento a ciascun Processo, la commissione dei Reati Presupposto.

2. PRINCIPI DI COMPORTAMENTO GENERALI

I Destinatari del Modello, nonché le Terze Parti coinvolte a qualsiasi titolo nelle Attività Sensibili, sono tenuti a:

- osservare le previsioni di legge esistenti in materia, nonché i principi generali richiamati nel Codice di Condotta di Gruppo e le procedure aziendali applicabili;

- rispettare i compiti, ruoli e responsabilità definiti dal sistema dei poteri, nonché dai contratti di servizi stipulati dalla Società in relazione allo svolgimento delle Attività Sensibili;
- astenersi dal tenere comportamenti tali da integrare i Reati Presupposto rilevanti per le Attività Sensibili;
- astenersi dal porre in essere comportamenti che, sebbene non risultino tali da configurare di per sé fattispecie di reato, possano integrare attività strumentali al compimento delle stesse, intendendosi per "strumentali" quelle attività che combinate con le attività direttamente sensibili, supportano la realizzazione del reato costituendone, quindi, la modalità di attuazione;
- comunicare tempestivamente alla Direzione aziendale ovvero al proprio referente aziendale (se esterni) eventuali deroghe ai presidi di controllo previsti nel presente Modello o nelle procedure aziendali.

Le Terze Parti sono inoltre tenute a informare tempestivamente il proprio referente aziendale nel caso in cui vengano a conoscenza di qualsiasi fatto che possa incidere in maniera rilevante sulla propria capacità di eseguire le attività esternalizzate in conformità con il contratto.

Infatti, dal momento che, allo stato, Unikeris non intrattiene rapporti di lavoro subordinato, la Società ha esternalizzato le attività aziendali mediante appositi contratti a (i) soggetti terzi (tra cui Terze Parti) e (ii) altre società del Gruppo (con il supporto di specifiche Funzioni aziendali).

Con riferimento all'esternalizzazione delle attività aziendali *sub.* i), le Terze Parti svolgono nei confronti della Società, a titolo esemplificativo e non esaustivo, attività relative alla distribuzione del Prodotto, gestione ed evasione degli ordini del Prodotto, partecipazione alle procedure indette dalla Pubblica Amministrazione per la fornitura del Prodotto.
Invece, relativamente all'esternalizzazione delle attività aziendali *sub.* ii), le società del Gruppo Chiesi primariamente coinvolte sono (a) Chiesi Limited che, tramite funzioni/dipendenti con sede in *UK*, fornisce alla Società una serie di servizi (es. servizio clienti, servizi di collegamento medico, affari medici, direzione, servizi finanziari, consulenza e assistenza per tutte le questioni relative alla gestione delle risorse umane, servizi legali, servizi di segreteria societaria, servizi di supporto e servizi normativi e garanzia della qualità) e (b) Chiesi Farmaceutici S.p.A. che, tramite funzioni/dipendenti con sede in Italia, fornisce servizi di supporto manageriale, la gestione degli adempimenti in materia fiscale relativi alla sede secondaria e di proprietà intellettuale, servizio clienti..

Oltre a quanto già delineato all'interno della Parte Generale, pgf. 8.3.4., i contratti di servizi devono regolamentare le modalità di esecuzione delle attività esternalizzate e impegnare le Terze Parti alla corretta esecuzione dell'attività nel rispetto della normativa vigente e delle disposizioni aziendali applicabili (es. Codice di Condotta, Codice di Interdipendenza dei Fornitori e *Policy Anti-Bribery* adottati dal Gruppo).

Nello svolgimento dei servizi esternalizzati, la Società è tenuta – ove possibile - a:

- verificare che gli incarichi conferiti alle Terze Parti siano redatti per iscritto e contengano, per quanto possibile, la clausola di rispetto delle disposizioni aziendali;
- prevedere nei contratti con le Terze Parti, a seconda della natura, della complessità e/o del valore dell'incarico, la possibilità da parte della Società di effettuare controlli – anche a campione – sull'attività prestata dalla controparte ai sensi del contratto;
- garantire che i rapporti con le Terze Parti che intervengono nella gestione delle Attività Sensibili avvengano nel rispetto delle leggi e delle normative vigenti;
- monitorare e valutare periodicamente le prestazioni delle Terze Parti.

3. PROCESSI SENSIBILI 231

3.1 *REGULATORY* E FARMACOVIGILANZA

Attività Sensibili

Il presente Processo comprende – in particolare - le seguenti Attività Sensibili:

- ❖ Gestione dei rapporti con le autorità competenti;
- ❖ Gestione dei reclami e delle segnalazioni sulla qualità del Prodotto;
- ❖ Gestione della segnalazione di eventuali reazioni avverse ai farmaci.

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di Reato Presupposto:

- Art. 24 – Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture;

- Art. 25 – Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio;
- Art. 25 *ter* - Reati societari.

Regole di comportamento

Nello svolgimento delle Attività Sensibili di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

Gestione dei rapporti con le autorità competenti, Gestione dei reclami e delle segnalazioni sulla qualità del Prodotto e Gestione della segnalazione di eventuali reazioni avverse ai farmaci

- gestire i rapporti con le Autorità esclusivamente tramite i soggetti muniti di idonei poteri e nell'assoluto rispetto delle leggi, delle normative vigenti, dei principi di trasparenza e correttezza;
- in caso di verifiche e ispezioni da parte di Autorità/Enti Pubblici esterni:
  - garantire la partecipazione a tali verifiche/ispezioni di almeno due soggetti differenti e dotati di adeguati poteri;
  - assicurare la tracciabilità di tutte le verifiche ispettive o sopralluoghi mediante la predisposizione di un apposito verbale o relazione;
  - trasmettere una comunicazione e-mail ai propri referenti relativa all'esito della verifica/ispezione;
  - in caso di rilievi da parte di Autorità/Enti Pubblici esterni, predisporre uno specifico piano di miglioramento che identifichi le non conformità e/o irregolarità osservate dagli ispettori durante la visita e definisca le eventuali azioni correttive, le funzioni responsabili e la tempistica per la relativa implementazione;
- nella gestione delle comunicazioni con Autorità:
  - operare, con correttezza ed imparzialità, attraverso i canali aziendali di comunicazione a ciò preposti;
  - rappresentare gli interessi e le posizioni della Società in maniera veridica, trasparente e coerente, evitando qualsiasi esposizione di informazioni o dichiarazioni non veritiere, incomplete o ingannevoli, al fine di procurare un indebito vantaggio alla Società;
  - nel caso in cui la documentazione da inviare sia prodotta - in tutto o in parte - con il supporto di Terze Parti o altri Destinatari del Modello, garantire che la selezione

delle stesse avvenga sempre nel rispetto dei requisiti di professionalità, indipendenza e competenza;

- in caso di richieste non conformi alle previsioni di legge da parte di un rappresentante di Autorità:
  - non dare seguito alla richiesta;
  - fornire tempestivamente informativa alla Direzione aziendale;
- attenersi ai provvedimenti stabiliti dalle autorità competenti in caso di reclami o segnalazioni relativi alla qualità del Prodotto;

Gestione della segnalazione di eventuali reazioni avverse ai farmaci

- rendere nota in modo chiaro ai soggetti coinvolti, che devono essere adeguatamente informati circa le modalità di segnalazione, la possibilità di effettuare segnalazioni relative a reazioni avverse del farmaco;
- garantire che le segnalazioni alle Autorità competenti:
  - avvengano tempestivamente e nel rispetto dei principi di diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere;
  - unitamente alla relativa modulistica e documentazione;
  - mediante accesso al database dell'Agenzia con impiego di *user ID* e *password* personali e da parte dei soggetti preventivamente identificati e autorizzati o da soggetti da questi appositamente delegati.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato sopra elencate; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

- presentare dichiarazioni o documentazione non veritiera ad Autorità o a rappresentanti delle stesse al fine di conseguire indebiti vantaggi (ad es. ottenere l'autorizzazione all'immissione in commercio o alla rimborsabilità di un farmaco);
- dare o promettere denaro o altra utilità a soggetti intermediari quale prezzo della propria mediazione illecita, affinché, sfruttando relazioni esistenti o asserite con i soggetti pubblici, esercitino un'influenza verso Autorità volta a condizionare l'azione delle stesse a vantaggio della Società;

- instaurare rapporti di collaborazione, in qualunque modo retribuiti, con dipendenti, collaboratori o stagisti di Autorità e adottare comportamenti volti a condizionare indebitamente il giudizio/parere delle stesse;
- assumere comportamenti contrari ai principi etico-deontologici adottati dalla Società, finalizzati a sollecitare l'*iter* procedimentale delle pratiche, anticipando le tempistiche di legge, ovvero l'ottenimento di informazioni che ricadono nella definizione di "riservatezza" di cui all'art. 3 del DM n. 353/1997 o che comunque sono escluse da diritto di accesso per normative specifiche;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a rappresentanti di Autorità o soggetti privati (es. pazienti, farmacie, distributori), anche a titolo personale o a seguito di illecite pressioni, in particolare al fine di evitare – rispettivamente – che venga dato seguito o che venga sporto un reclamo o effettuata una segnalazione;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a rappresentanti di Autorità, anche a titolo personale o a seguito di illecite pressioni, al fine di influenzare la classificazione dei difetti oggetto di reclamo/segnalazione, sottostimandone la gravità e pericolosità;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a rappresentanti di Autorità, anche a titolo personale o a seguito di illecite pressioni, al fine di evitare – a seguito di un reclamo/segnalazione – che si proceda alla diffusione di comunicazioni relative a difetti del Prodotto sia attraverso il portale delle Autorità che attraverso i media e che vengano adottati provvedimenti verso la Società;
- occultare o distruggere corrispondenza o ogni altra documentazione prodotta relativa alle Attività Sensibili descritte nel presente Processo.

Controlli specifici

Con specifico riferimento alla *Gestione dei reclami e delle segnalazioni sulla qualità del Prodotto* e alla *Gestione della segnalazione di eventuali reazioni avverse ai farmaci* sono effettuati i seguenti controlli (a cura del responsabile della Funzione *Quality* di Chiesi Ltd, Funzione Farmacovigilanza di Chiesi US e Funzione *Customer Service* di Chiesi Farmaceutici S.p.A., per quanto di rispettiva competenza):

- ✓ verifica della completezza, accuratezza e correttezza delle segnalazioni ricevute dai clienti;
- ✓ garantire che tutte le segnalazioni ricevute dai clienti siano trasmesse tempestivamente ai siti di produzione per le conseguenti attività di verifica.

Controlli procedurali

Si considerano applicabili le seguenti procedure aziendali, adottate dalla Società e/o dal Gruppo, che regolamentano e disciplinano le Attività Sensibili oggetto del presente Processo:

- *Quality Policy*;
- *Quality Manual*;
- *Site Master File*;
- UKUNK-SOP-QA-0001, *Supply of the Product as an unlicensed medicine*.

Si precisa che le regole, i divieti e i controlli specifici di cui sopra applicabili all'Attività Sensibile *Gestione dei rapporti con le autorità competenti* si estendono – anche laddove non espressamente previsto – a tutte le altre Attività Sensibili in cui siano coinvolte Pubbliche Amministrazioni e/o Pubblici Ufficiali.

3.2 GESTIONE DELLE ATTIVITÀ DI COMMERCIALIZZAZIONE/FORNITURA DEL PRODOTTO

Attività Sensibili

Il presente Processo comprende – in particolare - le seguenti Attività Sensibili:

- Gestione delle richieste di fornitura del prodotto e delle *unsolicited requests* da parte degli HCP ;
- Qualificazione clienti;
- Partecipazione a gare pubbliche e private e negoziazioni dirette;
- Gestione della fornitura/logistica di prodotto;
- Gestione delle attività di importazione e dei relativi adempimenti doganali i.v.a.

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di Reato Presupposto:

- Art. 24 – Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture;

- Art. 25 – Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio;
- Art. 25 *ter* - Reati societari;
- Art. 25 *octies* - Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio;
- Art. 25 *quinquesdecies* - Reati tributari.

Regole di comportamento

Nello svolgimento delle Attività Sensibili di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

Gestione delle richieste di fornitura del prodotto e delle unsolicited requests da parte degli HCP

- garantire la massima trasparenza ed evitare qualsiasi condotta lesiva della concorrenza;
- evitare comportamenti idonei a ledere gli altrui diritti di proprietà industriale e/o intellettuale;

Qualificazione clienti

- rispettare la normativa nazionale e sovranazionale in materia di qualificazione dei clienti;
- tenere condotte tali da garantire il libero e corretto svolgimento del commercio nonché una lecita concorrenza nel rispetto della fede pubblica;
- tenere condotte tali da non compromettere la buona fede della controparte;
- garantire che il Prodotto fornito dalla Società possa essere venduto ai clienti / pazienti richiedenti;
- formalizzare i criteri in base ai quali un cliente / paziente può essere "cancellato" dalle liste interne della Società;

Partecipazione a gare pubbliche e private e negoziazioni dirette

- identificare in modo chiaro i ruoli e le responsabilità delle Funzioni coinvolte nell'Attività Sensibile, con particolare riferimento a (i) l'attuazione degli adempimenti previsti dalle leggi in vigore, (ii) l'individuazione dei soggetti deputati alla predisposizione dei documenti da trasmettere al soggetto pubblico e (iii) l'ottenimento dell'autorizzazione preventiva da parte della Società in merito alla partecipazione a gare pubbliche e private da parte di terzi;

- monitorare costantemente le gare/trattative private e le negoziazioni dirette con la PA con particolare riferimento alle fasi evolutive dei procedimenti di gara e delle negoziazioni;
- monitorare il rispetto da parte di terzi (i.e. Interlabo) dei termini contrattuali definiti con la Società relativamente alle modalità di partecipazione della stessa alle gare/trattative private e/o negoziazioni dirette con la PA.

Gestione della fornitura/logistica di prodotto

- garantire che tutti i Fornitori di logistica coinvolti nella gestione dell'Attività Sensibile conservino il Prodotto secondo specifiche condizioni di stoccaggio e ne assicurino il corretto mantenimento prima della relativa commercializzazione/fornitura;
- intrattenere rapporti esclusivamente con Fornitori che garantiscano elevati *standard* in materia di adozione di misure antinfortunistiche idonee a tutela dei propri lavoratori e che garantiscano ai propri lavoratori condizioni di lavoro sane, sicure e dignitose.

Gestione delle attività di importazione e dei relativi adempimenti doganali i.v.a.

- garantire il rispetto di tutte le norme di legge in vigore con riferimento alle attività di importazione del Prodotto, anche in materia fiscale e doganale;
- avvalersi del supporto di spedizionieri, doganalisti e/o agenzie esterne esperte sulle tematiche doganali con cui sottoscrivere uno specifico mandato;
- garantire che il Prodotto (e/o la sua confezione e/o l'etichettatura) non possa subire alterazioni, modifiche, manipolazioni e/o manomissioni tali da compromettere la qualità dello stesso;
- garantire l'individuazione delle Funzioni competenti coinvolte nelle attività relative alle fasi di gestione dei rapporti con la dogana (predisposizione della documentazione necessaria, verifica della completezza e accuratezza, ed approvazione della stessa);
- garantire che le figure che gestiscono gli adempimenti doganali per conto della Società siano dotate delle necessarie autorizzazioni/certificazioni (es. iscrizione nell'albo unico nazionale per i doganalisti e certificato A.E.O. gli spedizionieri internazionali);
- garantire che, nell'espletamento delle attività da parte degli spedizionieri/doganalisti/agenzie vengano assicurate: a) trasparenza e tracciabilità delle attività svolte, e b) un'attività di reportistica interna; in particolare, devono essere tracciate tutte le operazioni di *import* svolte;

- predisporre e presentare le dichiarazioni in dogana, anche tramite soggetti terzi, fornendo dati ed informazioni veritieri (es. codice tariffario, origine, valore, quantità, etc.), e adempiere correttamente al versamento i.v.a.;
- definire le modalità di notifica di eventuali irregolarità alle autorità competenti, in conformità alle disposizioni normative vigenti connesse al singolo accadimento;
- garantire che i terzi che supportano la Società informino tempestivamente il referente aziendale di qualsiasi fatto che possa incidere in maniera rilevante sulla propria capacità di eseguire le attività esternalizzate in conformità alla normativa vigente; in particolare, gli spedizionieri / doganalisti /agenzie dovranno informare la Società nel caso di anomalie riscontrate nella gestione delle pratiche;
- gestire i rapporti con le autorità doganali (ovvero con le altre Pubbliche Amministrazioni competenti) esclusivamente tramite i soggetti muniti di idonei poteri e nell'assoluto rispetto delle leggi, delle normative vigenti, dei principi di trasparenza e correttezza;
- in caso di verifiche e ispezioni da parte delle autorità doganali:
  - assicurare la tracciabilità di tutte le verifiche ispettive o sopralluoghi mediante la predisposizione di un apposito verbale o relazione interna;
  - trasmettere una comunicazione *e-mail* ai propri referenti relativa all'esito della verifica/ispezione;
  - in caso di rilievi da parte delle autorità, predisporre uno specifico piano di miglioramento che identifichi le non conformità e/o irregolarità osservate dagli ispettori durante la visita e definisca le eventuali azioni correttive;
- nella gestione delle comunicazioni con le autorità:
  - operare, con correttezza ed imparzialità, attraverso i canali aziendali di comunicazione a ciò preposti;
  - rappresentare gli interessi e le posizioni della Società in maniera veridica, trasparente e coerente, evitando qualsiasi esposizione di informazioni o dichiarazioni non veritiere, incomplete o ingannevoli, al fine di procurare un indebito vantaggio alla Società;
  - nel caso in cui la documentazione da inviare sia prodotta - in tutto o in parte - con il supporto di soggetti terzi (consulenti, periti tecnici, etc.), garantire che la selezione degli stessi avvenga sempre nel rispetto dei requisiti di professionalità, indipendenza e competenza;

- prevedere che tutti i Fornitori coinvolti nella gestione delle Attività Sensibili (tra cui spedizionieri/doganalisti/agenzie) siano soggetti a un processo di valutazione consistente in: i) una verifica in materia di compliance e ii) una verifica in materia HSE.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

- presentare dichiarazioni o documentazione non veritiera a Pubbliche Amministrazioni o a rappresentanti della stessa al fine di conseguire indebiti vantaggi;
- dare o promettere denaro o altra utilità a soggetti intermediari quale prezzo della propria mediazione illecita, affinché, sfruttando relazioni esistenti o asserite con i soggetti pubblici, esercitino un'influenza verso Pubbliche Amministrazioni volta a condizionare l'azione della stessa a vantaggio della Società;
- instaurare rapporti di collaborazione, in qualunque modo retribuiti, con dipendenti, collaboratori o stagisti di Pubbliche Amministrazioni e adottare comportamenti volti a condizionare indebitamente il giudizio/parere degli stessi;
- porre in essere accordi restrittivi della concorrenza con partners e/o clienti e/o distributori terzi, anche per tramite degli agenti;
- vendere i prodotti a prezzi particolarmente vantaggiosi al fine di ottenere indebiti vantaggi sui concorrenti;
- commercializzare/fornitura prodotti che non siano in possesso delle relative autorizzazioni, anche doganali e/o non siano stati sottoposti agli specifici controlli di qualità previsti dalla normativa applicabile e da quella aziendale;
- effettuare forniture di prodotti di qualità diversa da quella dichiarata o pattuita;
- porre in essere comportamenti idonei a ledere gli altrui diritti di proprietà industriale e intellettuale;
- svolgere attività promozionali e di *marketing* sul Prodotto;
- occultare o distruggere corrispondenza o ogni altra documentazione prodotta relativa alle Attività Sensibili di cui al presente Processo;

Partecipazione a gare pubbliche e private e negoziazioni dirette

- promettere o versare somme di denaro, beni in natura o altre utilità o benefici indebiti ai soggetti pubblici o privati affinché sia accettata l'offerta della Società nell'ambito di una gara d'appalto o di una negoziazione diretta;
- comunicare o inserire nei software della Pubblica Amministrazione dati falsi in relazione alla Società e/o ai prodotti da essa commercializzati/forniti;
- accedere abusivamente o danneggiare i *software* della stazione appaltante;
- modificare artatamente la documentazione relativa alle caratteristiche del prodotto, al fine di renderlo conforme alle specifiche richieste del bando;
- accordarsi con il *partner* o il cliente al fine di ottenere indebiti benefici dalla partecipazione al bando;
- intercedere illecitamente presso un pubblico ufficiale od una controparte privata al fine di far ottenere l'aggiudicazione della gara al cliente o *partner*;
- impedire o turbare una gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni, ovvero allontanare gli offerenti, mediante violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti;
- turbare il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente mediante violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione;

Gestione delle attività di importazione e dei relativi adempimenti doganali i.v.a.

- omettere o ritardare la presentazione della dichiarazione doganale, ovvero, gestire impropriamente le formalità doganali attraverso l'indicazione di informazioni non veritiere circa la quantità, qualità o il valore delle merci;
- sottrarsi fraudolentemente al pagamento delle obbligazioni doganali;
- sottrarre la merce al sistema di controllo della dogana istituito per l'accertamento e la riscossione dei diritti di confine, non dichiarandola alla stessa oppure occultandola o falsificando i documenti di trasporto e/o commerciali/di fornitura (es. attribuendo alla merce, all'interno dei documenti doganali, un valore ridotto rispetto a quello che viene normalmente indicato per analoga merce proveniente dal medesimo paese di origine o nell'ipotesi in cui, all'interno dei documenti certificanti il trasporto, venga indicato un quantitativo di merce inferiore a quello in esubero accertato in sede di visita da parte del delegato al controllo, ecc.);

- usare impropriamente merci estere importate/esportate in franchigia e con riduzione dei diritti di confine, destinandole o utilizzandole in modo differente da quello per il quale la franchigia o la riduzione erano state concesse;
- introdurre nello Stato merci estere in sostituzione di merci nazionali o nazionalizzate spedite in circolazione;
- sottrarre merci al pagamento di diritti di confine attraverso la manipolazione artificiosa delle stesse ovvero attraverso l'utilizzo di mezzi fraudolenti.

Controlli specifici

Con specifico riferimento alla *Gestione delle richieste di fornitura del prodotto e delle unsolicited requests da parte degli HCP* e alla

Qualificazione clienti sono effettuati i seguenti controlli (a cura del responsabile della Funzione Quality di (Chiesi Ltd.):

- ✓ verifiche volte alla qualificazione iniziale e al mantenimento della qualificazione nel tempo in capo a ciascun cliente / paziente

Con specifico riferimento alla *Partecipazione a gare pubbliche e private e negoziazioni dirette* sono effettuati i seguenti controlli):

- ✓ rilascio di previa ed espressa autorizzazione a favore di terzi (i.e. Interlabo) per la partecipazione a gare pubbliche e private in nome e per conto di Unikeris;
- ✓ controllo sui documenti da presentare per la gara/trattativa privata/negoziazione diretta/offerta (*check list* e documentazione richiesta), al fine di verificare la completezza e accuratezza della documentazione;
- ✓ verifica della corrispondenza di quanto fornito alla Pubblica Amministrazione rispetto a quanto indicato nei bandi pubblici (anche in termini di modalità, tempistiche, quantità e qualità);
- ✓ verifica delle gare a cui la Società ha partecipato e/o intende partecipare mediante l'analisi della reportistica periodica predisposta dal Procuratore Speciale;

Con specifico riferimento alla *Gestione della fornitura/ logistica di prodotto* e alla *Gestione delle attività di importazione e dei relativi adempimenti doganali i.v.a.* sono effettuati i seguenti controlli (a cura del responsabile della Funzione *Tax* competente):

- ✓ monitoraggio normativo, anche con l'ausilio di consulenti esterni, al fine di riscontrare sopraggiunte novità normative e/o giurisprudenziali e/o nuove *best practice* rilevanti in materia di *import/export*;
- ✓ verifiche volte alla qualificazione iniziale e al mantenimento della qualificazione nel tempo in capo a ciascun Fornitore/Terza Parte, eventualmente anche mediante svolgimento di *audit on-site*;
- ✓ controllo circa la congruità delle somme corrisposte agli spedizionieri/doganalisti/agenzie (tariffario per servizi prestati, rimborso spese, oneri doganali etc.);
- ✓ controllo sulle operazioni doganali svolte dai soggetti esterni in nome e per conto della Società; in particolare, la Società monitora le attività degli spedizionieri/doganalisti/agenzie in relazione all'efficacia del servizio svolto;
- ✓ verifica delle dichiarazioni doganali, nonché della correttezza e accuratezza dei dati inseriti all'interno delle stesse.

Controlli procedurali

Si considerano applicabili le seguenti procedure aziendali, adottate dalla Società e/o dal Gruppo, che regolamentano e disciplinano le Attività Sensibili oggetto del presente Processo:

- *Quality Manual*;
- *Qualification of Supplier, Customer and Service Providers* (UKUNK-WI-QA-0001);
- *Supply of the Product as an unlicensed medicine* (UKUNK-SOP-QA-0001).

3.3 GESTIONE DEGLI AFFARI LEGALI E SOCIETARI

Attività Sensibili

Il presente Processo comprende – in particolare - le seguenti Attività Sensibili:

- ❖ Gestione dei rapporti/contratti *intercompany*/infragruppo;
- ❖ Contenzioso, accordi transattivi e consulenze legali.

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di Reato Presupposto:

- Art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio;
- Art. 25 *ter* – Reati societari;
- Art. 25 *octies* - Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio;
- Art. 25 *decies* - Induzione a rendere dichiarazioni mendaci all'autorità giudiziaria;
- Art. 25 *quinquiesdecies* - Reati tributari;
- Art. 24 *ter* - L. 146/06 - Delitti di criminalità organizzata (anche transnazionale).

Regole di comportamento

Nello svolgimento delle Attività Sensibili di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

Gestione dei rapporti/contratti intercompany/infragruppo

- garantire che i rapporti *intercompany* siano regolati tramite specifici contratti, redatti secondo gli *standard* infra-Gruppo definiti – volti a garantire, tra gli altri, il rispetto anche di normative non di diretta attinenza legale (quali, ad esempio, la correttezza sotto il profilo fiscale della determinazione dei prezzi, trasparenza contabile e separatezza patrimoniale) – e disciplinanti, tra gli altri:
  - il dettaglio delle attività oggetto di contratto ed i servizi erogati;
  - i ruoli e le responsabilità delle parti;
  - i compensi pattuiti ed i relativi parametri per la determinazione dei corrispettivi;
- assicurarsi che i contratti stipulati con società del Gruppo siano sottoscritti da soggetti dotati di idonei poteri;
- garantire la tracciabilità di tutte le operazioni con le società del Gruppo mediante l'archiviazione di tutta la documentazione rilevante;
- garantire che i rapporti *intercompany* siano improntati ai principi di correttezza e trasparenza, nel rispetto del principio di autonomia delle società del Gruppo e dei principi di corretta gestione, in modo da garantire la tutela degli stakeholders di tutte le società del Gruppo;
- predisposizione di una adeguata reportistica al vertice aziendale avente ad oggetto la sottoscrizione di nuovi contratti *intercompany*

Contenzioso, accordi transattivi e consulenze legali

- assicurare che, nei rapporti con l'Autorità Giudiziaria, le Funzioni aziendali competenti prestino una fattiva collaborazione e rendano dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti;
- assicurare la comunicazione tempestiva alla Società circa la convocazione ricevuta da parte dell'Autorità Giudiziaria e gli eventuali sviluppi successivi del procedimento in cui il soggetto chiamato a rendere dichiarazioni all'Autorità Giudiziaria è coinvolto in qualità di persona avente facoltà di non rispondere, al fine di permettere alla Società stessa di prendere gli opportuni provvedimenti volti ad assicurare l'indipendenza e autonomia del soggetto medesimo e di tutelare al tempo stesso la Società da potenziali rischi in termini di responsabilità amministrativa degli enti;
- informare tempestivamente la Direzione aziendale circa eventuali contenziosi che coinvolgono (anche solo potenzialmente) la Società di cui si venisse a conoscenza nell'esercizio delle proprie attività;
- garantire che, nei rapporti con l'Autorità Giudiziaria, coloro i quali dovessero risultare indagati o imputati in un procedimento penale, anche connesso, inerente all'attività lavorativa prestata nella Società, esprimano liberamente le proprie rappresentazioni dei fatti o esercitino la facoltà di non rispondere accordata dalla legge;
- assicurare l'assoluta autonomia del soggetto chiamato a rendere dichiarazioni all'Autorità Giudiziaria, nella scelta del legale di sua fiducia cui rivolgersi, ovvero salvaguardare l'indipendenza e la libertà nell'esprimersi davanti all'Autorità Giudiziaria;
- in caso di verifiche e ispezioni da parte di autorità giudiziarie:
  - predisporre un apposito verbale o relazione interna al fine di assicurare la tracciabilità di tutte le verifiche ispettive o sopralluoghi;
  - garantire la partecipazione a tali verifiche/ispezioni di almeno due soggetti appartenenti a Funzioni aziendali differenti e dotati di adeguati poteri;
  - trasmettere una comunicazione *e-mail* ai propri referenti relativa all'esito della verifica/ispezione;
  - in caso di rilievi da parte dell'autorità giudiziaria, predisporre uno specifico piano di miglioramento da parte del soggetto preposto o di un soggetto da questi appositamente incaricato che identifichi le non conformità e/o irregolarità osservate dagli ispettori durante la visita e definisca le eventuali azioni correttive;
- selezionare i legali esterni sulla base di comprovata capacità sulla materia oggetto della consulenza;

- applicare, ove possibile e opportuno, un principio di rotazione dei consulenti legali, tenendo in debita considerazione la specifica *expertise* dei professionisti;
- vincolare il legale esterno attraverso apposite clausole contrattuali che prevedano i) il rispetto delle prescrizioni dettate dal Codice di Interdipendenza dei Fornitori e dalla *Policy Anti-Bribery* e ii) il diritto della Società, in caso di inadempimento, di risolvere unilateralmente il contratto stipulato e di richiedere il risarcimento per eventuali danni causati da condotte in contrasto con le suddette prescrizioni;
- partecipare attivamente alla gestione delle attività condotte dai legali esterni, anche mediante interlocuzioni periodiche con i legali esterni, invio tempestivo della documentazione, partecipazione allo svolgimento dell'attività istruttoria, revisione delle bozze degli atti ecc.;
- valutare – di concerto con i legali esterni - le azioni legali da intraprendere (attive o passive) al fine di adottare la strategia più adeguata anche in considerazione della natura, dell'oggetto e del valore della causa;
- richiedere ai legali esterni una relazione periodica da trasmettere alla Direzione aziendale sull'andamento dei contenziosi, nonché sui possibili scenari di sviluppo e sulle eventuali problematiche del giudizio;
- registrare i contenziosi in essere, con l'indicazione delle informazioni più rilevanti (attore, convenuto, oggetto, importo richiesto, legali rappresentanti, status del contenzioso).

In conformità con la recente giurisprudenza, nel caso in cui la Società venisse individuata quale ente incolpato nell'ambito di un procedimento ex Decreto 231 e in tale procedimento il legale rappresentante della Società fosse direttamente coinvolto in qualità di indagato per il reato presupposto dell'illecito amministrativo ascritto all'ente, la nomina del difensore della Società deve essere effettuata da un soggetto diverso (munito degli appositi poteri) da detto legale rappresentante.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

Gestione dei rapporti/contratti intercompany/infragruppo

- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio mediante utilizzo di fatture per operazioni inesistenti emesse da terzi),

finalizzate alla creazione di disponibilità che potrebbero potenzialmente essere destinate alla commissione di illeciti, con particolare riferimento alle condotte di natura corruttiva;

- attribuire fittiziamente la disponibilità o la titolarità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzioni patrimoniali.;

Contenzioso, accordi transattivi e consulenze legali

- adottare comportamenti contrari alle leggi in sede di incontri formali ed informali, anche a mezzo di legali esterni e Consulenti, per indurre l'autorità giudiziaria a favorire indebitamente gli interessi della Società;
- adottare comportamenti contrari alle leggi in sede di ispezioni/controlli/verifiche da parte dell'autorità giudiziaria, per influenzarne il giudizio/parere nell'interesse della Società, anche a mezzo di legali esterni e Consulenti;
- presentare dichiarazioni o documentazione non veritiera all'Autorità Giudiziaria o a rappresentanti della stessa al fine di conseguire indebiti vantaggi (ad es. ottenere favoritismi nell'ambito di un procedimento civile/penale);
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a rappresentanti dell'Autorità Giudiziaria, Pubblica Amministrazione (es. GdF) o soggetti privati (es. Consulenti legali), anche a titolo personale o a seguito di illecite pressioni, in particolare al fine di conseguire indebiti vantaggi per la Società;
- dare o promettere denaro o altra utilità a soggetti intermediari quale prezzo della propria mediazione illecita, affinché, sfruttando relazioni esistenti o asserite con i soggetti pubblici, esercitino un'influenza verso l'Autorità Giudiziaria volta a condizionare l'azione delle stesse a vantaggio della Società;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione in relazione al tipo di incarico contrattualmente affidato;
- instaurare rapporti di collaborazione, in qualunque modo retribuiti, con dipendenti, collaboratori o stagisti dell'Autorità Giudiziaria e adottare comportamenti volti a condizionare indebitamente il giudizio/parere degli stessi;
- coartare od indurre, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della Società, la volontà dei Destinatari di rispondere all'Autorità Giudiziaria o di avvalersi della facoltà di non rispondere;
- accettare, nei rapporti con l'Autorità Giudiziaria, denaro o altra utilità, anche attraverso Consulenti della Società;

- promettere o offrire denaro o qualsivoglia utilità ovvero ricorrere all'uso di violenza o minaccia, al fine di indurre un soggetto chiamato a testimoniare a non rilasciare dichiarazioni ovvero a rilasciare dichiarazioni false davanti all'Autorità Giudiziaria, qualora tali dichiarazioni possano essere utilizzate all'interno di un processo penale;
- effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri sia direttamente, sia tramite consulenti o soggetti terzi che agiscono in nome e per conto della Società;
- accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Autorità Giudiziaria che possano influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società;
- con riguardo alla gestione dei contenziosi con i privati ed alla gestione dei rapporti con gli arbitri (nell'ambito della composizione di liti mediante designazione di un arbitro o di un collegio arbitrale) è fatto divieto di sollecitare/indurre/ricevere, direttamente o per il tramite di consulenti o altri soggetti terzi, un indebito vantaggio (es. induzione della controparte a transare in modo favorevole per la Società) ovvero accettare l'offerta o la promessa, per compiere o astenersi dal compiere un atto in violazione dei propri doveri legali, professionali o contrattuali relativi all'attività di competenza (es. transare in modo sfavorevole per la Società);
- indurre con dazioni o promesse di pagamento o altre utilità persone chiamate a rendere dichiarazioni in un procedimento ad agire nell'interesse o a vantaggio della Società;
- effettuare prestazioni o pagamenti in favore di legali esterni, Consulenti, periti o altri soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- tenere comportamenti discriminatori e/o di ritorsione nei confronti del soggetto chiamato a rendere dichiarazioni all'Autorità Giudiziaria a seguito delle dichiarazioni rese all'autorità

Controlli specifici

Con specifico riferimento alla *Gestione dei rapporti/contratti intercompany/infragruppo* sono effettuati i seguenti controlli (a cura del responsabile della Funzione Legal di Chiesi Farmaceutici S.p.A. e Chiesi Ltd, a seconda dei casi):

- ✓ verifica della sottoscrizione dei contratti che regolano i rapporti *intercompany* da parte di soggetti dotati di idonei poteri;

Con specifico riferimento alla *Gestione del Contenzioso, accordi transattivi e consulenze legali* sono effettuati i seguenti controlli (a cura del responsabile della Funzione Legal):

- ✓ monitoraggio costante delle azioni legali penali, civili, amministrative e tributarie, attive o passive;
- ✓ monitoraggio delle prestazioni eseguite dai legali esterni al fine di verificare le modalità di svolgimento delle attività stesse;
- ✓ verifica della sottoscrizione di tutta la documentazione e gli atti prodotti nell'ambito della gestione dei contenziosi e rapporti con l'Autorità Giudiziaria da parte di soggetti dotati di idonei poteri;
- ✓ verifica della sottoscrizione di eventuali proposte per accordi transattivi/arbitrati da parte di soggetti dotati di idonei poteri;
- ✓ verifica dell'assenza di potenziali conflitti di interesse tra i professionisti incaricati della gestione del contenzioso e le parti coinvolte nel contenzioso/accordo transattivo;
- ✓ verifiche circa la coerenza dei corrispettivi riconosciuti a consulenti/professionisti legali rispetto alle attività concretamente svolte.

Controlli procedurali

Nello svolgimento delle attività per conto di UNIKERIS, Chiesi Farmaceutici S.p.A. applica - per quanto applicabili - le relative SOPs che regolamentano tali attività.

3.4 *INTELLECTUAL PROPERTY*

Attività Sensibili

Il presente Processo comprende – in particolare - la seguente Attività Sensibile:

- ❖ Gestione dei marchi e dei brevetti (relativi al Prodotto).

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di Reati Presupposto:

- Art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio;
- Art. 25 *bis* - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;

- Art. 25 *bis* 1 - Delitti contro l'industria e il commercio;
- Art. 25 *quinquesdecies* - Reati tributari.

Regole di comportamento

Nello svolgimento dell'Attività Sensibile di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

- osservare rigorosamente tutte le leggi e i regolamenti che disciplinano la gestione delle opere dell'ingegno;
- promuovere il corretto uso di tutte le opere dell'ingegno;
- gestire i rapporti con i licenziatari nel rispetto della normativa vigente, con un adeguato grado di formalizzazione, nonché nel rispetto dei principi di trasparenza e correttezza;
- disciplinare le modalità di autorizzazione per la concessione delle licenze nel rispetto della normativa e dei regolamenti vigenti;
- adottare comportamenti che siano conformi ai principi etici adottati dal Gruppo in materia di politica fiscale;
- ricorrere ad adeguate misure di manleva per eventuali rivendicazioni, azioni legali e richieste di risarcimento presentate da terzi, a seguito di violazioni di brevetti o di richieste di brevetto, di marchi o di modelli depositati e di diritti di proprietà industriale e intellettuale attinenti a prodotti comprati da terzi;
- informare tempestivamente la Direzione aziendale in caso di eventuali rivendicazioni/azioni legali/richieste di risarcimento presentate da terzi aventi ad oggetto il presunto utilizzo illecito delle opere dell'ingegno;
- osservare rigorosamente gli adempimenti fiscali derivanti dalla gestione dei diritti di proprietà intellettuale e industriale, anche con il supporto di consulenti esterni specializzati;
- gestire i rapporti con le autorità pubbliche competenti al rilascio / rinnovo dei marchi e brevetti esclusivamente tramite i soggetti muniti di idonei poteri e nell'assoluto rispetto delle leggi, delle normative vigenti, dei principi di trasparenza e correttezza;
- nella gestione delle comunicazioni con le autorità pubbliche:
  - operare, con correttezza ed imparzialità, attraverso i canali aziendali di comunicazione a ciò preposti;
  - rappresentare gli interessi e le posizioni della Società in maniera veridica, trasparente e coerente, evitando qualsiasi esposizione di informazioni o

dichiarazioni non veritiere, incomplete o ingannevoli, al fine di procurare un indebito vantaggio alla Società;

- nel caso in cui la documentazione da inviare sia prodotta - in tutto o in parte - con il supporto di soggetti terzi (consulenti, periti tecnici, etc.), garantire che la selezione degli stessi avvenga sempre nel rispetto dei requisiti di professionalità, indipendenza e competenza;

- in caso di richieste non conformi alle previsioni di legge da parte di un rappresentante di autorità pubbliche:
  - non dare seguito alla richiesta;
  - fornire tempestivamente informativa alla Direzione aziendale.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

- riprodurre abusivamente, imitare o manomettere marchi, segni distintivi, brevetti, disegni industriali o modelli in titolarità di terzi;
- fare uso, in ambito industriale e/o commerciale, di marchi, segni distintivi, brevetti, disegni industriali o modelli contraffatti da soggetti terzi;
- utilizzare nomi o segni distintivi idonei a creare confusione con nomi o segni distintivi legittimamente usati da altri, o falsificare i prodotti di un competitor, o compiere con qualsiasi altro mezzo atti idonei a produrre confusione con i prodotti e con l'attività di un concorrente;
- adoperare, in qualsiasi forma o modalità, opere dell'ingegno di cui la Società non detenga la proprietà esclusiva e/o legittimo titolo all'uso, potendo conoscerne l'esistenza con ordinaria e qualificata diligenza;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, mirate alla falsificazione o alterazione delle evidenze documentali e\o di registrazione a supporto delle dichiarazioni tributarie e/o fiscali volte a ottenere risparmi di imposta mediante alterazione dei dati relativi alle *royalties* percepite in relazione a marchi aziendali;
- introdurre nel territorio dello Stato per farne commercio, detenere per vendere o mettere in qualunque modo in circolazione prodotti con marchi o segni distintivi contraffatti o alterati da soggetti terzi;

- dare o promettere denaro o altra utilità a soggetti intermediari quale prezzo della propria mediazione illecita, affinché, sfruttando relazioni esistenti o asserite con i soggetti pubblici, esercitino un'influenza verso le autorità pubbliche competenti volta a condizionare l'azione della stessa a vantaggio della Società;
- instaurare rapporti di collaborazione, in qualunque modo retribuiti, con dipendenti, collaboratori o stagisti delle autorità pubbliche competenti e adottare comportamenti volti a condizionare indebitamente il giudizio/parere degli stessi;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a rappresentanti di autorità pubbliche competenti o soggetti privati (es. Consulenti, agenti brevettuali, etc.), anche a titolo personale o a seguito di illecite pressioni, in particolare al fine di ottenere indebiti vantaggi;
- occultare o distruggere corrispondenza o ogni altra documentazione relativa all'Attività Sensibile descritta nel presente Processo.

Controlli specifici

Sono effettuati i seguenti controlli (a cura del responsabile della Funzione *Corporate Intellectual Property – Patents* e *Global Trademarks, Domains & Brand Protection* di Chiesi Farmaceutici S.p.A., per quanto di rispettiva competenza):

- ✓ verifica di anteriorità prima di procedere alla registrazione/rinnovo presso gli uffici competenti, al fine di evitare di incorrere in marchi/domini/brevetti già oggetto di deposito;
- ✓ verifica di legittimità sulla regolare titolarità del marchio/dominio/brevetto da parte del soggetto cedente, nel caso di acquisizioni o licenze d'uso;
- ✓ inserimento, in determinate categorie di contratti di acquisizione di prodotti tutelati da diritti di proprietà intellettuale, di specifiche clausole con cui la controparte:
  - attesta di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi o che siano questi oggetto di libero utilizzo;
  - attesta che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o di concessione in uso non violano alcun diritto di proprietà industriale in capo a terzi;

- si impegna a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione;
- si impegna al rispetto della normativa vigente sul diritto d'autore e proprietà intellettuale, nonché sul trattamento delle informazioni privilegiate (clausole di riservatezza e confidenzialità);
- si impegna a rispettare il Codice di Interdipendenza dei Fornitori;

✓ approvazione finale da parte della Direzione aziendale, per il rilascio di licenze a soggetti terzi.

La Funzione Finance di Chiesi Ltd e/o la Funzione *Tax* di Chiesi Farmaceutici S.p.A., a seconda dei casi, verifica inoltre che le previsioni contrattuali relative alle royalties siano corrispondenti ai dati rappresentati nelle dichiarazioni fiscali.

3.5 *INFORMATION TECHNOLOGY*

Attività Sensibili

Il presente Processo comprende – in particolare - la seguente Attività Sensibile:

❖ Gestione e utilizzo strumenti informatici.

Si precisa che gli strumenti informativi e i relativi applicativi a disposizione dei soggetti che svolgono attività a favore di Unikeris sono di proprietà di altre società del Gruppo (es. Chiesi Farmaceutici S.p.A., Chiesi Ltd, etc.) e sono gestiti secondo le modalità e le procedure stabilite a livello aziendale e/o di Gruppo

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di reato:

- Art. 24 - Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.);
- Art. 24 *bis* - Delitti informatici;
- Art. 25 *novies* – Delitti in materia di violazione del diritto d'autore.

Regole di comportamento

Nello svolgimento dell'Attività Sensibile di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

- operare nel pieno rispetto delle disposizioni aziendali disciplinanti la sicurezza dei sistemi IT;
- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- astenersi da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati aziendali e altrui;
- accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e provvedere, entro le scadenze prestabilite, alla modifica periodica delle password;
- attivare ogni misura ritenuta necessaria per la protezione del sistema informatico, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione;
- adottare misure di protezione dei documenti elettronici aventi efficacia legale da inviare all'esterno;
- segnalare alla Direzione aziendale eventuali incidenti di sicurezza informatica fornendo tutte le informazioni e l'eventuale documentazione necessaria per una corretta valutazione del caso;
- utilizzare esclusivamente software di cui si possiede regolare licenza;
- rispettare i diritti d'autore di terzi utilizzando esclusivamente codici sorgenti originali o per i quali si sia precedentemente ottenuta una specifica autorizzazione da parte del titolare dei relativi diritti;
- garantire che i server siano ospitati in locali appositamente dedicati e messi in sicurezza e che l'accesso a tali locali sia riservato al solo personale autorizzato;
- assicurare che i *backup* dei dati ospitati su server siano salvati con frequenza periodica e che i supporti siano adeguatamente messi in sicurezza ovvero conservati e protetti anche tramite sistemi ignifughi;
- garantire l'accesso ai sistemi informativi aziendali e agli applicativi gestionali ai soli soggetti autorizzati attraverso l'assegnazione di *password* e *user ID*;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- utilizzare le risorse informatiche aziendali rispettando le misure di sicurezza stabilite dalla Società (modifica e custodia delle password, utilizzo dei sistemi di protezione quali antivirus, etc.) evitando comportamenti che possano comprometterne il loro corretto funzionamento o generare danni a soggetti terzi.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

- porre in essere condotte che possano compromettere la riservatezza e l'integrità delle informazioni e dei dati della Società e qualsiasi altra condotta diretta a superare o aggirare le protezioni del sistema aziendale altrui;
- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- modificare artificiosamente, ovvero alterare o eliminare il contenuto di comunicazioni relative a sistemi informatici o telematici;
- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, l'alterazione del suo funzionamento (il divieto include la trasmissione di *virus* con lo scopo di danneggiare i sistemi informativi di enti concorrenti);
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici (il divieto include l'intrusione non autorizzata nel sistema informativo di società concorrente, con lo scopo di alterare informazioni e dati di quest'ultima);
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici relativi alla sanità o comunque di interesse pubblico ;
- distruggere, deteriorare, danneggiare, cancellare, alterare o sopprime informazioni al fine di rendere in tutto o in parte inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento;

- porre in essere, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse della Società, comportamenti di qualsivoglia natura atti a ledere diritti di proprietà intellettuale altrui;
- duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale - o comunque per trarne profitto - programmi per elaboratori, banche dati, opere a contenuto letterario, musicale, multimediale, cinematografico, artistico per i quali non siano stati assolti gli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi al suo esercizio;
- duplicare abusivamente un'opera di ingegno (ad es. *software* od applicativi gestionali), al fine di sfruttarli senza il pagamento della relativa licenza;
- installare sulle dotazioni informatiche aziendali *software* non autorizzati o comunque utilizzare software non autorizzati o sprovvisti di licenza d'uso;
- intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
- diffondere - tramite reti telematiche - un'opera dell'ingegno o parte di essa;
- accedere abusivamente ai sistemi informatici o telematici aziendali e/o di soggetti pubblici o privati (es. società concorrenti) anche al fine di acquisire illecitamente, alterare o cancellare dati e/o informazioni;
- accedere senza autorizzazione a sistemi informativi utilizzati dalla Pubblica Amministrazione intervenendo con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi per ottenere e/o modificare gli stessi a vantaggio della Società;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita o comunque mettere in circolazione - al fine di trarne profitto - beni/opere realizzati usurpando il diritto d'autore o brevetti di terzi;
- utilizzare i beni aziendali e, in particolare, le dotazioni informatiche aziendali, per commettere o indurre alla commissione di reati o per perseguire qualsiasi finalità contraria a norme di legge vigenti o che possa costituire una minaccia per l'ordine pubblico, la tutela dei diritti umani o il buon costume;
- occultare o distruggere corrispondenza o ogni altra documentazione prodotta in relazione alle Attività Sensibili di cui al presente Processo.

Controlli specifici

Sono effettuati i seguenti controlli (a cura delle Funzioni IT di Chiesi Farmaceutici S.p.A. e Chiesi Ltd, a seconda dei casi):

- ✓ sono definiti i criteri e le modalità per la creazione delle *password* di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (es. lunghezza minima della *password*, regole di complessità, scadenza);
- ✓ l'aggiornamento delle *password* di accesso ai sistemi informativi è richiesto periodicamente, in conformità alla normativa vigente;
- ✓ le nuove utenze sono attivate sulla base di modalità predefinite e sono definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- ✓ sono effettuati controlli periodici sull'effettiva attività degli *account* e, in caso di inattività dell'utenza, si procede al blocco degli stessi;
- ✓ sono monitorati l'effettiva disattivazione delle credenziali e di tutte le utenze attive per i soggetti che terminano la prestazione lavorativa a favore di Unikeris, con particolare riferimento ai anche soggetti terzi rispetto alla Società;
- ✓ sono previsti, laddove necessario, meccanismi di protezione dei files relativi alle attività svolte da Unikeris, quali ad esempio *password*, conversione dei documenti in formato non modificabile.

Controlli procedurali

Nello svolgimento delle attività per conto di UNIKERIS, Chiesi Farmaceutici S.p.A. applica - per quanto applicabili - le relative SOPs che regolamentano tali attività.

3.6 FINANZA E FISCALITÀ

Attività Sensibili

Il presente Processo comprende – in particolare – le seguenti Attività Sensibili:

- ❖ Gestione della fatturazione elettronica attiva;
- ❖ Gestione della contabilità;
- ❖ Gestione degli adempimenti fiscali derivanti dalle attività di fatturazione attiva (es. IRES, IRAP, 770, etc.).

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di reato:

- Art. 24 *bis* - Delitti informatici;

- Art. 25 *ter* - Reati societari;
- Art. 25 *octies* - Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio;
- Art. 25 *quinquesdecies* - Reati tributari.

Regole di comportamento

Nello svolgimento delle Attività Sensibili di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

- garantire che le principali novità normative in materia fiscale siano tempestivamente diffuse al personale coinvolto nella gestione delle fiscalità, fornendo un'adeguata formazione del personale addetto alle tematiche fiscali e un costante aggiornamento sulle novità tributarie al fine di monitorare l'evoluzione dei relativi rischi;
- porre la massima attenzione nello svolgimento di attività con soggetti terzi (es. transazioni finanziarie) ed attività infragruppo (contratti di acquisto e/o di vendita; gestione dei flussi finanziari, investimenti) al fine di individuare e/o prevenire eventuali operazioni/situazioni idonee ad integrare una delle ipotesi delittuose in esame;
- osservare la normativa antiriciclaggio e comunicare alla Direzione aziendale le violazioni delle relative disposizioni di cui vengano a conoscenza nell'esercizio dei propri compiti o di cui abbiano altrimenti notizia;
- rispettare gli adempimenti (sia in termini di dichiarazioni che di pagamenti) e le scadenze definite dalla normativa fiscale in materia di imposte dirette ed indirette;
- tenere e conservare correttamente le scritture contabili rilevanti ai fini fiscali;
- trasporre correttamente i dati relativi alle scritture contabili rilevanti ai fini fiscali nelle dichiarazioni annuali e periodiche funzionali all'assolvimento delle imposte;
- liquidare correttamente le imposte periodiche;
- tenere traccia delle eventuali compensazioni di crediti tributari richiamati in fase di dichiarazione fiscale o di versamento;
- regolarizzare tempestivamente eventuali irregolarità rilevate nel corso dei controlli svolti internamente;
- garantire il corretto trattamento fiscale delle componenti di reddito, detrazioni e deduzioni secondo quanto previsto dalla normativa fiscale;
- consentire l'accesso al sistema di *remote banking* al solo personale dotato di apposite credenziali al fine di consentire la corretta liquidazione delle imposte secondo le procure in vigore;

- riservare l'accesso al sistema informativo fiscale della Società a soggetti in possesso delle necessarie abilitazioni e permessi;
- provvedere ad un continuo allineamento tra i profili utente assegnati ed il ruolo ricoperto all'interno della Società;
- mantenere nei rapporti con l'amministrazione finanziaria un comportamento chiaro, trasparente, diligente e collaborativo, fornendo tutti i dati e le notizie eventualmente richieste;
- assicurare che i soggetti preposti ad intrattenere rapporti con l'amministrazione fiscale e la Guardia di Finanza per le questioni concernenti l'accertamento e la liquidazione delle imposte effettuino l'attività di *reporting* periodico e quella che si renda necessaria in virtù di circostanze contingenti, al fine di garantire ai soggetti muniti dei necessari poteri la possibilità di intraprendere le necessarie attività correttive. In particolare, in caso di verifiche e ispezioni da parte dell'amministrazioni finanziaria / fiscale:
  - garantire la partecipazione a tali verifiche/ispezioni di almeno due soggetti appartenenti a Funzioni aziendali differenti e dotati di adeguati poteri;
  - assicurare la tracciabilità di tutte le verifiche ispettive o sopralluoghi mediante la predisposizione di un apposito verbale o relazione interna;
  - trasmettere una comunicazione e-mail ai propri referenti relativa all'esito della verifica/ispezione;
  - in caso di rilievi, predisporre uno specifico piano di miglioramento che identifichi le non conformità e/o irregolarità osservate dagli ispettori durante la visita e definisca le eventuali azioni correttive;
- nella gestione delle comunicazioni con l'amministrazione finanziaria / fiscale:
  - operare, con correttezza ed imparzialità, attraverso i canali aziendali di comunicazione a ciò preposti;
  - rappresentare gli interessi e le posizioni della Società in maniera veridica, trasparente e coerente, evitando qualsiasi esposizione di informazioni o dichiarazioni non veritiere, incomplete o ingannevoli, al fine di procurare un indebito vantaggio alla Società;
  - nel caso in cui la documentazione da inviare sia prodotta - in tutto o in parte - con il supporto di soggetti terzi (consulenti, periti tecnici, etc.), garantire che la selezione degli stessi avvenga sempre nel rispetto dei requisiti di professionalità, indipendenza e competenza;

- in caso di richieste non conformi alle previsioni di legge da parte di un rappresentante di un'amministrazione finanziaria / fiscale:
  - non dare seguito alla richiesta;
  - fornire tempestivamente informativa alla Direzione aziendale.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione in relazione al tipo di incarico contrattualmente affidato;
- effettuare pagamenti a qualsivoglia soggetto che non trovino adeguata giustificazione nel rapporto contrattuale;
- porre in essere trasferimenti di denaro qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione (anche a titolo di concorso) di riciclaggio, ricettazione, impiego di denaro, beni o utilità di provenienza illecita o autoriciclaggio;
- creare fondi a fronte di pagamenti non giustificati;
- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare conti aperti in Paesi esteri ove ciò non sia correlato alla sottostante attività;
- trasferire denaro contante o detenere/trasferire libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera per importi, anche frazionati, complessivamente pari o superiori ai limiti normativi vigenti;
- accettare assegni emessi da soggetti che non siano debitori nei confronti della Società, a meno che gli stessi non siano stati contrattualmente identificati dal debitore;
- emettere assegni bancari e postali, ad eccezione di quelli circolari, per importi pari o superiori ai limiti normativi vigenti che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare pagamenti in contanti, eccetto per le particolari tipologie di acquisto rientranti nella piccola cassa e comunque entro gli importi massimi previsti dai limiti normativi vigenti e dal sistema documentale aziendale;
- ricevere somme attraverso trasferimenti di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore in euro o in valuta estera, diversi dai

titoli azionari, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore ai vigenti limiti normativi;

- effettuare qualsiasi operazione che possa ostacolare l'identificazione della provenienza del denaro (es. giroconto o acquisto di titoli o strumenti finanziari) senza giustificato motivo;
- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio mediante utilizzo di fatture per operazioni inesistenti emesse da terzi), finalizzate alla creazione di disponibilità che potrebbero potenzialmente essere destinate alla commissione di illeciti;
- effettuare operazioni, anche con società del Gruppo, al fine di eludere le normative fiscali nonché disposizioni di legge in materia di misure di prevenzione patrimoniali o contrabbando;
- registrare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione parziale o non corretta e veritiera della realtà riguardo alla situazione economica, patrimoniale, finanziaria e fiscale della Società e del Gruppo nonché al fine di celare operazioni volte ad attribuire fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità;
- alterare o distruggere documenti ed informazioni finanziarie e contabili, ad esempio attraverso accessi non autorizzati ai sistemi informativi aziendali o altre azioni idonee allo scopo predetto;
- omettere di comunicare dati e informazioni imposte dalla legge, con riguardo alla situazione economica, patrimoniale e finanziaria della società e del Gruppo, anche quando destinati alle autorità di vigilanza cui è soggetta l'attività aziendale, nonché omettere di dar corso con sollecitudine all'invio di tali dati e della documentazione eventualmente richiesta dalle predette autorità;
- porre in essere qualsiasi comportamento che sia di ostacolo alle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità di vigilanza;
- porre in essere qualsiasi comportamento – mediante l'utilizzo di sistemi informatici e/o telematici - volto ad evadere, o consentire ad altri di evadere, le imposte sui redditi o sul valore aggiunto, nonché dal compiere operazioni simulate o dall'avvalersi di altri mezzi fraudolenti;
- evadere le imposte sui redditi o sul valore aggiunto;
- avvalersi, emettere o rilasciare fatture o altri documenti per operazioni inesistenti;

- indicare in fatture o altri documenti relative alle imposte sui redditi o sul valore aggiunto elementi passivi fittizi ovvero elementi attivi per un ammontare inferiore a quello effettivo;
- compiere operazioni simulate oggettivamente o soggettivamente, o comunque avvalersi di documenti falsi o di altri mezzi fraudolenti;
- consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto;
- occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi;
- indicare in una delle dichiarazioni annuali relative alle imposte sui redditi o sul valore aggiunto elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti;
- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione parziale o non corretta e veritiera della realtà riguardo alla situazione economica, patrimoniale, finanziaria e fiscale della Società;
- effettuare qualsiasi operazione che possa ostacolare l'identificazione della provenienza del denaro senza giustificato motivo;
- effettuare operazioni, anche con società del Gruppo, al fine di eludere le normative fiscali;
- presentare dichiarazioni o documentazione finanziaria e/o tributaria non veritiera ad un ente pubblico o a rappresentanti dello stesso al fine di conseguire indebiti vantaggi

accedere abusivamente a sistemi informativi della Pubblica Amministrazione con l'obiettivo di (a) alterare il funzionamento e/o i programmi del sistema telematico, (b) alterare i dati e le informazioni in esso contenute (dichiarazioni fiscali, attestazioni o autocertificazioni dirette ad enti pubblici, documenti creati con l'ausilio di strumenti di firma digitale, documentazione relativa alla pratica di assunzione trasmessa agli enti preposti INAIL, INPS, ecc.) o (c) danneggiare e/o distruggere i dati in essi contenuti

Controlli specifici

Sono effettuati i seguenti controlli (a cura del responsabile della Funzione *Tax* di Chiesi Farmaceutici S.p.A. e Funzione *Finance* di Chiesi Ltd, a seconda dei casi):

- ✓ verifica circa la legittimità, correttezza, completezza, accuratezza, coerenza e congruità delle informazioni contabili;
- ✓ verifica della corretta applicazione dei principi contabili di riferimento, nonché della normativa vigente, nel processo di contabilizzazione delle imposte correnti e differite;

- ✓ verifica della completezza e correttezza dei dati necessari al calcolo delle imposte, della correttezza del calcolo delle imposte, nonché della completa e corretta registrazione contabile;
- ✓ verifica delle attività e/o operazioni contabili poste in essere al fine di impedire la creazione di disponibilità extracontabili (ad esempio mediante l'utilizzo di fatture per operazioni inesistenti emesse da terzi), ovvero finalizzate alla creazione di "fondi neri" o di "contabilità parallele";
- ✓ monitoraggio dell'evoluzione della normativa di riferimento, al fine di garantire l'adeguamento alle novità normative in materia fiscale, e delle tempistiche da rispettare per le comunicazioni, denunce e adempimenti nei confronti dell'Amministrazione Finanziaria, al fine di evitare ritardi e imprecisioni nella presentazione delle stesse;
- ✓ verifica circa il rispetto dei termini e delle modalità previsti dalla normativa applicabile per la predisposizione delle dichiarazioni fiscali periodiche e per i conseguenti versamenti relativi alle imposte sui redditi e sul valore aggiunto;
- ✓ approvazione delle dichiarazioni fiscali da parte del Rappresentante Legale della Società.

Controlli procedurali

Nello svolgimento delle attività per conto di UNIKERIS, Chiesi Farmaceutici S.p.A. applica - per quanto applicabili - le relative SOPs che regolamentano tali attività.

3.7 ACQUISTI NON CORE

Attività Sensibili

Il presente Processo comprende – in particolare - la seguente Attività Sensibile:

- ❖ Acquisti di servizi.

Reati Presupposto

Il presente Processo è volto alla prevenzione delle seguenti famiglie di Reato Presupposto:

- Art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio;
- Art. 25 *ter* - Reati societari;
- Art. 25 *octies* - Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio;
- Art. 25 *quinquesdecies* - Reati tributari.

Regole di comportamento

Nello svolgimento dell'Attività Sensibile di cui al presente Processo, tutti i Destinatari sono tenuti ad osservare le regole di comportamento di seguito indicate:

- garantire che i rapporti con Fornitori/Consulenti avvengano nell'assoluto rispetto di leggi, normative vigenti e principi di lealtà, correttezza, chiarezza e trasparenza;
- creare una specifica anagrafica Fornitori/Consulenti al fine di raccogliere e censire tutte le informazioni rilevanti e necessarie allo svolgimento delle attività;
- autorizzare gli ordini/intrattenere rapporti contrattuali solo con Fornitori/Consulenti in possesso di adeguati requisiti di affidabilità, integrità ed etica;
- nelle eventuali situazioni di conflitto di interesse, segnalare tempestivamente tali circostanze alla Direzione aziendale ed astenersi dall'intervenire nel processo operativo/decisionale riguardante il rapporto con il Fornitore/Consulente;
- documentare le motivazioni che hanno determinato la selezione del Fornitore/Consulente, curando l'archiviazione della relativa documentazione;
- motivare adeguatamente e per iscritto l'eventuale ricorso a "fornitore unico" derivante da esigenze specifiche *(know how* esclusivo, vincoli tecnologici, emergenze, gara andata deserta, esperienza comprovata rispetto alla materia, etc.), nonché qualunque ulteriore deroga alle ordinarie modalità di sottoscrizione e/o gestione dei contratti con i Fornitori/Consulenti, che devono in ogni caso essere sempre formalmente approvate in conformità con i prescritti livelli autorizzativi;
- procedere alla valutazione delle offerte ricevute secondo criteri improntati alla trasparenza e – per quanto possibile – alla limitazione dei criteri di soggettività e al principio di rotazione dei Fornitori/Consulenti;
- garantire la tracciabilità dell'iter di selezione del Fornitore/Consulente, attraverso l'archiviazione della relativa documentazione di supporto;
- garantire che le forniture siano autorizzate, verificate e sottoscritte dai soggetti dotati di idonei poteri;
- garantire che i rapporti con i Fornitori/Consulenti siano formalizzati tramite specifici accordi scritti, sottoscritti da soggetti muniti di idonei poteri;
- vincolare il Fornitore/Consulente attraverso apposite clausole contrattuali che prevedano i) il rispetto delle prescrizioni dettate dal Codice di Interdipendenza dei Fornitori e/o dalla *Policy Anti-Bribery* e ii) il diritto della Società, in caso di inadempimento,

di risolvere unilateralmente il contratto stipulato e di richiedere il risarcimento per eventuali danni causati da condotte del Fornitore in contrasto con le suddette prescrizioni;

- inserire nei contratti con i Fornitori/Consulenti apposite clausole che prevedano tra l'altro:
  - la responsabilità di questi ultimi anche per l'operato di eventuali sub-Fornitori in riferimento ai diritti di terzi;
  - che l'impresa interessata dichiari di essere dotata delle autorizzazioni richieste dalla legge per lo svolgimento della propria attività;
  - che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto;
- specificare nei contratti con i Fornitori/Consulenti la descrizione dei servizi dovuti dalla controparte, il corrispettivo, i termini e le condizioni di pagamento;
- generare ed emettere gli ordini di acquisto esclusivamente tramite il sistema aziendale ed in accordo al sistema documentale vigente, al fine di consentirne la tracciabilità;
- registrare con accuratezza e tempestività tutte le transazioni di acquisto, verificando preventivamente che siano state autorizzate sulla base dei poteri autorizzativi formalizzati;
- accettare solo servizi esplicitamente ordinati e comunque conformi alle specifiche contenute nell'ordine di acquisto;
- assicurare che tutti i pagamenti a Fornitori o appaltatori siano effettuati solamente se adeguatamente supportati da contratto o ordine o a seguito di un iter autorizzativo interno predefinito;
- eseguire pagamenti verso i Fornitori/Consulenti direttamente ed esclusivamente su conti a questi intestati, previamente verificati e inseriti nel sistema aziendale.

Divieti

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001; più in particolare, a titolo esemplificativo e non esaustivo, è vietato:

- instaurare rapporti con soggetti che si rifiutino o mostrino reticenza nel fornire informazioni rilevanti ai fini della loro corretta, effettiva e completa conoscenza o rispetto ai quali sussistano elementi di sospetto in ragione anche dell'eventuale operatività in Paesi non collaborativi, ovvero che facciano richiesta od offrano prestazioni che, pur

astrattamente vantaggiose per la Società, presentino profili di irregolarità o che possano porre in essere comportamenti in contrasto con leggi e regolamenti in materia di circolazione dei capitali e dei beni, fiscale o contabile;

- instaurare rapporti con Fornitori/Consulenti qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione di Reati, ad esempio in caso di notizia o fondato sospetto di condotte corruttive, azioni o supporto ad attività terroristiche o attività di riciclaggio perpetrate dal Fornitore/Consulente;
- effettuare prestazioni in favore di Fornitori/Consulenti che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e riconoscere loro compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- impegnare la Società con ordini/contratti verbali;
- concludere contratti con i Fornitori/Consulenti che prevedano la domiciliazione bancaria dei pagamenti riguardanti la prestazione in Paesi diversi da quello in cui il Fornitore ha stabilito la propria sede legale/operativa/commerciale;
- effettuare pagamenti in favore di Fornitori/Consulenti diversamente da quanto stabilito contrattualmente;
- effettuare pagamenti in contanti, su conti correnti cifrati o non intestati al Fornitore/Consulente o diversi da quelli previsti dal contratto;
- effettuare pagamenti in Paesi diversi da quello di residenza/sede legale/operativa/commerciale del Fornitore/Consulente;
- effettuare pagamenti non adeguatamente documentati;
- dare o promettere denaro o altra utilità a soggetti intermediari quale prezzo della propria mediazione illecita, affinché, sfruttando relazioni esistenti o asserite con i soggetti pubblici, esercitino un'influenza verso la Pubblica Amministrazione volta a condizionare l'azione pubblica a vantaggio della Società;
- offrire, promettere o erogare denaro o altra utilità ad un soggetto privato, ovvero ad un soggetto da questi segnalato, o autorizzare chiunque ad eseguire, direttamente o indirettamente, tali attività, al di fuori del normale iter autorizzativo del processo di approvvigionamento;
- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio mediante utilizzo di fatture per operazioni inesistenti emesse da terzi),

finalizzate alla creazione di disponibilità che potrebbero potenzialmente essere destinate alla commissione di illeciti, con particolare riferimento alle condotte di natura corruttiva;

- occultare o distruggere corrispondenza o ogni altra documentazione prodotta in relazione all'Attività Sensibile di cui al presente Processo.

Controlli specifici

Sono effettuati i seguenti controlli (a cura del responsabile della Funzione richiedente la prestazione):

- ✓ comparazione di più offerte/preventivi;
- ✓ verifica circa l'attendibilità tecnica e professionale dei Fornitori/Consulenti, nonché il possesso dei requisiti di onorabilità, professionalità, regolarità contributiva e solidità finanziaria;
- ✓ verifica del possesso da parte del Fornitore/Consulente di certificazioni in corso di validità: (i.e. ISO 9001, ISO 14001, OHSAS 18001, Rating di legalità, ecc.) e/o iscrizioni ad albi;
- ✓ verifica circa l'iscrizione da parte del Fornitore alla *White List* (per Fornitori cui la stessa è applicabile – i.e. trasportatori, smaltitori, ecc.)
- ✓ verifica circa l'esistenza delle specifiche autorizzazioni dei Fornitori/Consulenti che svolgono attività per le quali le stesse sono richieste;
- ✓ rilascio da parte del Fornitore/Consulente di specifica autodichiarazione in merito alla non sussistenza di situazioni pregiudizievoli (coinvolgimento in indagini e/o pronunce di condanna per reati di cui al Codice penale, ecc. nonché di conflitti d'interesse con la Società);
- ✓ valutazione circa potenziali conflitti di interesse con il Fornitore/Consulente;
- ✓ verifica dell'approvazione della richiesta di acquisto da parte di soggetti dotati di idonei poteri;
- ✓ laddove previsto dalle procedure interne applicabili, garantire che i rapporti con i Fornitori o Consulenti/professionisti siano formalizzati tramite specifici accordi scritti, sottoscritti da soggetti muniti di idonei poteri;
- ✓ verifica della congruità dei corrispettivi richiesti dai Fornitori/Consulenti rispetto alla prestazione e alle condizioni di mercato;
- ✓ rilascio del benestare alla fatturazione e successivo pagamento solo nei casi in cui le forniture/prestazioni siano conformi agli accordi intercorsi con il Fornitore/Consulente;

- ✓ verifica circa la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatario/ordinante e controparti effettivamente coinvolte.

Controlli procedurali

Nello svolgimento delle attività per conto di UNIKERIS, Chiesi Farmaceutici S.p.A. applica - per quanto applicabili - le relative SOPs che regolamentano tali attività.

4. FLUSSI INFORMATIVI

Ai fini dell'efficace vigilanza sull'attuazione del Modello i Destinatari, in ragione del proprio ruolo e delle proprie responsabilità, sono tenuti alla trasmissione dei flussi informativi verso l'Organismo di Vigilanza aventi ad oggetto lo svolgimento delle Attività Sensibili.

Processo	Area / Funzione Aziendale	Flusso Informativo	Periodicità
Acquisti non *core*	Responsabile Funzione richiedente	Anomalie emerse in sede di verifica delle fatture ricevute	Ad evento
		Elenco prestazioni di servizi per importi superiori a Euro 15.000,00	Annuale
Affari legali e societari	Funzione Legal di Chiesi Farmaceutici S.p.A. o di Chiesi Ltd, per quanto di rispettiva competenza	Provvedimenti e/o notizie aventi ad oggetto l'esistenza di un procedimento penale, anche nei confronti di ignoti, relativo a fatti di interesse per la Società	Ad evento
		Provvedimenti e/o notizie aventi ad oggetto l'esistenza di procedimenti amministrativi o controversie civili di rilievo relativi a richieste o iniziative di Autorità indipendenti, dell'amministrazione finanziaria, di amministrazioni locali, ai contratti con la Pubblica Amministrazione, alle richieste e/o gestione di finanziamenti pubblici	Ad evento

Processo	Area / Funzione Aziendale	Flusso Informativo	Periodicità
		Operazioni finanziarie/societarie significative o atipiche che possano essere a rischio di commissione di un Reato Presupposto	Ad evento
		Richieste di assistenza legale inoltrate alla Società dalla direzione aziendale in caso di avvio di procedimenti penali o civili nei loro confronti	Ad evento
		Ogni modifica che intervenga sul sistema delle deleghe adottato dalla Società	Ad evento
		Qualsiasi intervento di natura ispettiva da parte di organismi pubblici (magistratura, Guardia di Finanza, altre Autorità, ecc.)	Ad evento
		Esiti delle verifiche ispettive condotte da Autorità esterne (i.e., GdF, Isp. Lav, C.C. ecc.), dai quali emergono significativi rilievi, nonché lo stato di attuazione dell'eventuale piano di azione elaborato al fine di eliminare detti rilievi	Ad evento

Processo	Area / Funzione Aziendale	Flusso Informativo	Periodicità

		Provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini o procedimenti, anche nei confronti di ignoti, per i reati ex D.Lgs. 231/2001 qualora tali indagini coinvolgano la Società o suoi Organi Sociali, Collaboratori, Consulenti, Partner, e Fornitori	Ad evento
		Informativa in merito alla sottoscrizione di contratti *intercompany*	Semestrale
		Informativa in merito a operazioni straordinarie all'interno del Gruppo che coinvolgono la Società	Ad evento
		Elenco degli ordini del giorno delle adunanze del Consiglio di Amministrazione della Società	Semestrale
Finanza e Fiscalità	Funzione *Tax* di Chiesi Farmaceutici S.p.A. e Funzione Finance di Chiesi Ltd, per quanto di rispettiva competenza	Qualsiasi intervento di natura ispettiva da parte di organismi pubblici (Amministrazione finanziaria e fiscale, Guardia di Finanza, ecc.).	Ad evento
		Eventuali comunicazioni della società di revisione concernenti aspetti che possono indicare lacune nel sistema dei controlli interni, osservazioni sul bilancio e/o fatti censurabili	Ad evento

Processo	Area / Funzione Aziendale	Flusso Informativo	Periodicità

		Segnalazioni da parte del Collegio Sindacale in merito ad eventuali anomalie/criticità riscontrate nello svolgimento dell'attività di valutazione e controllo sull'adeguatezza dell'assetto organizzativo e del sistema di controllo interno della Società	Ad evento
		Anomalie emerse in sede di verifica delle fatture	Ad evento
		Attestazione di avvenuto invio delle dichiarazioni fiscali	Annuale
		Informativa in merito all'utilizzo di crediti tributari in compensazione per importi superiori ad € 50.000	Annuale
		Copia del bilancio di esercizio approvato	Annuale
		Comunicazione di verifiche fiscali in corso	Semestrale
		Comunicazione degli esiti delle verifiche fiscali	Semestrale
Gestione delle attività di commercializzazione/fornitura del Prodotto	Funzione *Quality* di Chiesi Ltd e/o Funzione Customer Service di Chiesi Farmaceutici S.p.A., per quanto di rispettiva competenza	Anomalie nella gestione del processo di qualificazione dei clienti	Ad evento
		Aggiornamenti inerenti ad eventuali cambiamenti organizzativi e/o di *business*	Ad evento
		Stipulazione di nuovi contratti di servizi o modifiche a contratti di servizi con fornitori per la gestione delle attività di fornitura del Prodotto nell'ambito del territorio italiano	Ad evento

Processo	Area / Funzione Aziendale	Flusso Informativo	Periodicità
	Funzione IEO&CM di Chiesi Farmaceutici S.p.A.	Qualsiasi intervento di natura ispettiva o richiesta di informazioni da parte di autorità doganali	Ad evento

	Funzione *Customer Service* di Chiesi Farmaceutici S.p.A.	Riepilogo delle gare pubbliche/private a cui la Società ha partecipato	Semestrale
	Funzione IEO&CM di Chiesi Farmaceutici S.p.A.	Attestazione di avvenuto adempimento degli adempimenti fiscali derivanti dalle attività di importazione	Semestrale
Information Technology	Funzione IT di Gruppo	Informativa su eventuali anomalie dei sistemi/strumenti informatici	Ad evento
Intellectual Property	Funzione *Corporate Intellectual Property – Patents e Global Trademarks, Domains & Brand Protection* di Chiesi Farmaceutici S.p.A., per quanto di rispettiva competenza	Qualsiasi intervento di natura ispettiva o richiesta di informazioni da parte di autorità competenti in materia di rilascio di marchi / brevetti	Ad evento
Processo	**Area / Funzione Aziendale**	**Flusso Informativo**	**Periodicità**
	Funzione *Legal* di Chiesi Farmaceutici S.p.A. o di Chiesi Ltd, per quanto di rispettiva competenza	Dettaglio delle variazioni/modifiche apportate ai contratti di licenza *intercompany*	

***Regulatory* e Farmacovigilanza**	Funzione *Quality* di Chiesi Ltd e Funzione Farmacovigilanza di Chiesi US, per quanto di rispettiva competenza	Qualsiasi intervento di natura ispettiva da parte di organismi pubblici (autorità regolatorie, autorità amministrative indipendenti, ecc.).	Ad evento
		Riepilogo dei reclami/segnalazioni inoltrati dal Fornitore alla Funzione competente	Semestrale

In ogni caso all'O.d.V. sono conferiti tutti i poteri ai sensi del Modello per richiedere in ogni momento ai Destinatari del Modello qualsiasi informazione, dato, documento, notizia. I Destinatari del Modello dovranno fornire senza indugio quanto richiesto all'O.d.V..

Resta altresì fermo il principio che ogni informazione, notizia o evento che ai sensi del Modello possa considerarsi utile ai fini dell'assolvimento dei compiti dell'O.d.V. dovrà essere trasmessa senza indugio all'O.d.V..

Inoltre, tutti i Destinatari coinvolti nello svolgimento delle Attività Sensibili sono tenuti a segnalare tempestivamente ogni informazione relativa a condotte illecite rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti o qualsiasi violazione del Modello.

Qualora si verifichino circostanze non espressamente regolamentate dalla presente Parte Speciale, che si prestino a dubbie interpretazioni e/o applicazioni da comportare deroghe all'applicazione della Parte Speciale, è fatto obbligo a ciascun Destinatario di comunicare tempestivamente il verificarsi delle suddette circostanze all'O.d.V..