ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

Pursuant to Italian Legislative Decree No. 231 of 8 June 2001

Approved by the Board of Directors on

21 December 2023

NEVA SGR

CONTENTS

1 LEGAL FRAMEWORK

1.1 The administrative liability scheme laid down in Legislative Decree No. 231/2001 for legal persons, companies and associations, including those without legal personality

By way of implementation of the delegation under Article 11 of Law No. 300 of 29 September 2000, on 8 June 2001 Legislative Decree No. 231 (hereinafter the "Decree" or also "Legislative Decree No. 231/2001") was adopted, aligning national legislation with the international conventions on the liability of legal persons. These are, specifically, the Brussels Convention on the protection of the European Union' financial interests of 26 July 1995, the Convention on the fight against corruption involving officials of the EU or officials of Member States of the European Union, signed in Brussels on 26 May 1997, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of 17 December 1997.

The Decree, which lays down "*Provisions on the administrative liability of legal persons, companies and associations, including those without legal personality*", introduced into the Italian legal order an administrative liability regime applying to Entities (meaning companies, associations, consortia, etc., hereinafter, "Entities") for a series of specified offences committed in the interest or to the advantage of the entity: (i) by natural persons holding representation, administration or management positions in the Entity or in a financially and functionally autonomous organisational unit belonging to the Entity; and by natural persons who exercise, also de facto, the management and control of the Entity, or (ii) by natural persons subject to the management or supervision of one of the above-mentioned persons. The list of "predicate offences" was recently expanded by the introduction of additional types of administrative breaches.

The Entity's liability is additional to that of the natural person who committed the offence, and is independent of it, as it also exists where the offender has not been identified or cannot be charged or where the offence is extinguished for a reason other than amnesty.

The administrative liability regime laid down in the Decree for prosecution of the offences specifically identified therein, applies to Entities which benefited from the offences or in whose interest the predicate offences - or administrative breaches - identified in the Decree were committed. The penalties applicable to the Entity may include fines, bans, confiscation, publication of the sentence and appointment of a special administrator. Prohibitory measures, which may have a more severe impact on the Entity than monetary penalties, consist in the suspension or revocation of licenses and concessions, prohibition on contracting with the public administration, prohibition on conducting business activities,

denial or revocation of funding and contributions, and the prohibition on advertising products and services.

The above-mentioned liability also applies to offences committed abroad, provided that the country in which the offence was committed does not initiate proceedings in respect of those offences and that the Entity has its head office in Italy.

1.2 The adoption of the organisational, management and control models as a means to exempt Entities from administrative liability

After establishing the administrative liability of Entities, in Article 6 the Decree provides that an Entity shall not be liable where it can prove that "*... adopted and effectively implemented, before the offence was committed, an appropriate organisation and management model to prevent offences of the kind that has occurred...*".

Article 6 also provides for creation of an internal control body within the Entity, tasked with "*monitoring the functioning, effectiveness and observance of the aforementioned model*", and with updating the model.

The "Organisational, Management and Control Model" adopted in accordance with Legislative Decree No. 231 of 8 June 2001 (hereinafter the "Model") has to meet the following requirements:

- identify the activities which may give rise to the offences listed in the Decree;
- define the procedures through which the Entity makes and implements decisions relating to the offences to be prevented;
- define procedures for managing financial resources to prevent offences from being committed;
- establish reporting obligations to the body responsible for monitoring Model operation and compliance;
- put in place an effective disciplinary system to punish non-compliance with the measures required by the Model.

If the offence is committed by persons holding a representative, administrative or management role in the Entity or one of its organisational units with financial and functional autonomy and by persons who, de facto or otherwise, manage and control the Entity, the Entity shall not be liable if it can prove that:

a) management had adopted and effectively implemented an appropriate organisational and management model to prevent offences of the kind that has occurred;

b) the task of monitoring the Model implementation, compliance and updating was entrusted to a corporate body of the Entity with independent powers of initiative and control;

c) the persons who committed the offence by fraudulently circumventing the Model;

d) there was no omission or insufficient control by the control body.

On the other hand, where the offence is committed by persons under the management or supervision of one of the above-mentioned persons, the Entity is liable if perpetration of the offence was made possible by non-performance of management and supervisory duties. Such non-performance shall be ruled out where the Entity, before the offence was committed, had adopted and effectively implemented an appropriate Model to prevent offences of the kind committed, based, of course, on a priori assessment.

Lastly, Article 6 of the Decree provides that the Model may be adopted on the basis of codes of conduct prepared by representative trade associations and submitted to the Ministry of Justice.

The Model of Neva SGR S.p.A., which also refers to the Model of the Parent Company Intesa Sanpaolo Spa, was prepared also having regard to the guidelines prepared by ABI and approved by the Ministry of Justice.

2 THE ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL OF NEVA SGR S.P.A.

2.1 The existing corporate tools underlying the Model

Neva SGR (hereinafter also the "Company") is a company belonging to the Intesa Sanpaolo Banking Group.

In preparing this Model, account was taken firstly of the current legislation and of the procedures and control systems already existing and implemented within Neva SGR, insofar as they were appropriate to also serve as measures for preventing offences and unlawful conduct in general, including those laid down in Legislative Decree 231/2001.

The organisational context of Neva SGR consists of the set of rules, structures and procedures that guarantee the functioning of the Company; it is therefore a structured system, defined and verified internally, also in order to comply with the regulatory provisions to which Neva SGR is subject directly as an Asset Management Company and indirectly as a Company belonging to the Intesa Sanpaolo Banking Group.

The Company is in fact subject to the supervision of the Bank of Italy and Consob, which carry out checks and controls on its operations and on aspects of its organisational structure, as required by the regulations. Moreover, as it is subject to the policy, governance and control activities exercised by the Parent Company, Neva SGR is required to comply with the provisions issued by Intesa Sanpaolo in connection with the governance activities of its investees.

This corpus of special rules, together with ongoing supervision by the competent Authorities constitute invaluable tools for preventing unlawful conduct in general, including the offences laid down in the specific legislation on the administrative liability of Entities.

The regulatory provisions also include the obligation for the Parent Company to prepare, pursuant to Legislative Decree No. 254/2016, the Consolidated Non-Financial Statement which, to the extent necessary to ensure an understanding of the Intesa Sanpaolo Group's business, its performance, its results and the impact it has produced, covers environmental, social, personnel, human rights topics, and the fight against active and passive bribery. The Statement must describe the company's management and organisational business model, including the organisational and management models adopted pursuant to Legislative Decree No. 231/2001, including with regard to the management of the aforementioned topics and the principal risks that arise from them.

The Company's already existing specific tools laying down the procedures through which the entity makes and implements decisions relating to the offences and breaches to be prevented include:

- the rules of corporate governance adopted in accordance with the relevant corporate laws and regulations;
- internal regulations and corporate policies;
- the Code of Ethics, Internal Code of Conduct and the Anti-corruption Guidelines of the Group;
- the internal control system;
- the powers and delegation system.

The rules, procedures and principles set out in the above-mentioned instruments are not described in detail in this Model but are integrated in the Model's broader organisational, management and control system which all internal and external parties are required to respect, in accordance with their relationship with the Company.

The following paragraphs are intended to provide an overview of the reference principles of the Code of Ethics, Internal Code of Conduct and Anti-corruption Guidelines, the internal control system, and the powers and delegation system.

2.1.1 Code of Ethics, Internal Code of Conduct and Anti-corruption Guidelines of the Group

In line with the importance assigned to ethical issues and to pursuing a conduct consistently inspired by criteria of rigour and integrity, the Company has implemented and adopted the Code of Ethics, Internal Code of Conduct and the Anti-corruption Guidelines of the Group.

The Code of Ethics is a voluntary, self-regulating tool that is an integral part of the Sustainability management model. It contains the mission, corporate values and the principles that regulate the relationships with the stakeholders, starting with the corporate identity. In certain particularly relevant areas (i.e. human rights, employment protection, environmental protection, the fight against corruption) the Code refers to rules and principles that are consistent with the best international standards.

The Group's Internal Code of Conduct, applicable to all Group Companies, is an intentionally lean set of rules. It includes general provisions – defining the essential rules of conduct for company representatives, staff and external collaborators who, in performing their duties, must operate with professionalism, diligence, honesty and correctness – and more specific provisions, such as the prohibition to engage in certain personal transactions.

With best international practices, the Anti-corruption Guidelines identify the principles, sensitive areas and define the Group's roles, responsibilities and the macro-processes for handling of the risk of corruption. They also provide for the Anti-Money Laundering function to undertake responsibility for governing this area and the Head of this department shall be the Corporate Anti-Corruption Officer.

2.1.2 The key features of the internal control system

Neva SGR, to ensure sound and prudent management, combines business profitability with an attentive risk-acceptance activity and an operating conduct based on fairness.

Therefore, the Company, in line with legal and supervisory regulations in force, has adopted an internal control system capable of identifying, measuring and continuously monitoring the risks typical of its business activities.

Neva SGR's internal control system is built around a set of rules, procedures and organisational structures aimed at ensuring compliance with Company strategies and the achievement of the following objectives:

- the effectiveness and efficiency of Company processes;
- the safeguarding of asset value and protection from losses;
- the reliability and integrity of accounting and management information;
- transaction compliance with the law, supervisory regulations as well as policies, plans, procedures and internal regulations.

The internal control system is characterised by a documentary infrastructure (regulatory framework) that provides organised and systematic access to the guidelines, procedures, organisational structures, and risks and controls within the business, incorporating both the Company policies and the instructions of the Supervisory Authorities, and the provisions of the law, including the principles laid down in Legislative Decree No. 231/2001.

The regulatory framework consists of "Governance Documents" that oversee the functioning of the Company (Articles of Association, Code of Ethics, Group Internal Code of Conduct, Group Regulations, Regulations for Related Party Transactions, Authorities and Powers, Policy and Guidelines of the Parent Bank, Organisational Manual, Functional Chart, etc.) and more strictly operational rules that regulate corporate processes, individual activities and related controls (Circulars, Processes, etc.).

More specifically, the Company rules set out organisational solutions that:

- ensure sufficient separation between the operational and control functions and prevent situations of conflict of interest in the assignment of responsibilities;
- are capable of adequately identifying, measuring and monitoring the main risks assumed in the various operational segments;
- enable the recording of every operational event and, in particular, of every transaction, with an adequate level of detail, ensuring their correct allocation over time;
- establish reliable information systems and suitable reporting procedures for the various management levels having control functions;

- ensure prompt reporting to the appropriate levels within the Company and the swift handling of any anomalies found by the business units, by the Internal Auditing Function or by other control functions.

Moreover, the Company's organisational solutions provide for control activities at all operational levels, which make it possible to identify responsibilities univocally and formally, in particular as concerns performing controls and correcting any irregularities found.

Following the indications provided by the Supervisory Authorities, Neva SGR has identified the following types of control described in detail within the Integrated Internal Control System Regulations:

- ***first level:*** line controls that aim to ensure correct application of the operations (e.g. hierarchical, systemic controls or controls on a sampling basis) which are, to the extent that is feasible, incorporated in IT procedures. These activities are carried out by the operating or business structures, including through units dedicated exclusively to control functions, which report to the managers of the structures themselves, or they are executed within the back office. The operating and business structures are the first line responsible parties for the risk management process and are required to comply with the operating limits assigned to them consistently with the risk objectives and the procedures which comprise the risk management process;
- ***second level:*** controls on risks and compliance that aim to ensure among other things: i) correct implementation of the risk management process, ii) compliance with the operating limits assigned to the various functions, iii) compliance of corporate operations with the laws, including self-regulation. The functions in charge of these controls are distinguished from the production functions and they participate in defining the risk and governance policies and the risk management process;
- ***third level:*** internal auditing, aimed at identifying anomalous trends, violations of procedures and regulations, as well as periodically assessing completeness, adequacy, functionality (in terms of efficiency and effectiveness) and the reliability of the internal control systems and the information system at pre-set intervals depending on the nature and intensity of the risks. It is performed by different structures which are independent from production structures.

The internal control system is periodically reviewed and adapted in relation to business developments and the reference context.

In particular, the Internal Audit Function, reporting directly to the Board of Directors, is entrusted, on the basis of a specific service contract, to the Head Office International Auditing and Wealth Management Department of the Parent bank. This function is also tasked with submitting to the Board of Directors, the Board of Statutory Auditors, the Top

Management and the Heads of the various Corporate Functions, proposals for possible improvements to risk management policies, measurement tools, processes and procedures.

2.1.3 The powers and delegation system

Pursuant to the Articles of Association, the Board of Directors is vested with all powers for the ordinary and extraordinary administration of the Company, and has delegated some of its powers to the Chief Executive Officer in order to ensure unity in the day-to-day management, in implementation of the Board's resolutions.

Furthermore, the Chief Executive Officer has defined the scope of the decision-making and spending powers conferred within the Company, in line with the organisational and management responsibilities assigned to the persons involved, also establishing the procedures and limits for the exercise of sub-delegations.

The power to sub-delegate is exercised through a constantly monitored transparent process, which is calibrated in accordance with the role and position of the sub-delegate, who in any case must always report back to the delegating function.

Moreover, the procedures for signing deeds, contracts, documents and internal and external correspondence are formalised, and the relevant signing powers are assigned to staff members jointly or severally.

All the Structures operate on the basis of the Organisational Manual, issued and brought to the attention of the Company, which defines the areas of competence and responsibility of each Corporate Function and sets out its powers of management autonomy.

Lastly, operational procedures, which define how the different corporate processes are to be performed are also disseminated throughout the Company by means of specific internal rules.

Therefore, all the main decision-making and implementing processes concerning Company operations are spelled out, observable and available to the entire corporate organisation.

2.2 The aims pursued by the Model

Although the corporate tools described in the preceding paragraphs would by themselves suffice to prevent the offences covered by the Decree, the Company decided to adopt a specific Organisational, Management and Control Model pursuant to the Decree, convinced that such model, besides being an important tool for raising the awareness of all those who operate on the Company’s behalf, leading them to operate with integrity and transparency, is also more effective in preventing the risk of the offences and the administrative breaches covered by the reference legislation being committed.

In particular, by adopting and regularly updating the Model, the Company pursues the following main aims:

- make all persons operating on the Company's account in the field of "sensitive activities" (i.e. those activities which, by their nature, are at risk for the offences identified in the Decree), aware of the fact that, should they breach the rules governing such activities, they might incur disciplinary and/or contractual sanctions, as well as criminal and administrative penalties;
- stress that any such unlawful conduct is strongly discouraged since (even where the Company would seem to benefit from it) such behaviour is in breach not only of the law, but also of the ethical principles which the Company intends to apply to all its activities;
- enable the Company, thanks to monitoring of the sensitive activity areas, to take swift action to prevent or fight any offences and punish conduct in breach of its Model.

2.3 Key Model components

Neva SGR's Model was prepared in accordance with the will of the legislator and was inspired by the model adopted by the Parent Company Intesa Sanpaolo, from which it drew its general approach, sharing its approach to the issues considered and its insights.

The key model components may be summarised as follows:

- identification of the activity areas at risk, i.e. the sensitive company activities where offences might occur, to be analysed and monitored;
- management of operational processes ensuring:
  - the separation of duties by adequately allocating responsibilities and establishing appropriate authorization levels in order to avoid functional overlaps or operating allocations that concentrate activities on a single person;
  - clear and formalised allocation of powers and responsibilities, expressly indicating the limits of those powers and consistent with the duties assigned and positions covered within the organisational structure;
  - appropriate procedures for performing the activities;
  - traceability of the acts, operations and transactions through an appropriate paper or electronic trail;
  - decision-making processes linked to previously established objective criteria (e.g.: the company keeps registers of approved suppliers, objective staff assessment and selection criteria are in place, etc.);
  - control and supervisory activities on company transactions are in place and traceable;

  - safety mechanisms are in place, providing appropriate data protection/access control to corporate data and assets;
- adequate rules of conduct are in place ensuring that corporate activities are carried out in compliance with the laws and regulations and safeguarding the company's assets;
- the responsibilities for the adoption, amendment, implementation and control of the Model have been defined;
- the Surveillance Body has been identified and specific duties of oversight on the Model's effective and proper functioning have been allocated;
- the information flows to the Surveillance Body have been defined;
- an effective disciplinary system has been put in place and implemented to punish non-compliance with the measures required by the Model;
- staff training and internal communication concerning the contents of the Decree and of the Model, and the associated compliance obligations.

2.4 Model structure

In defining this "Organisational, Management and Control Model", Neva SGR has taken into account the new organisational structure assumed by the Company.

The approach followed by Neva SGR in defining the Model was characterised by the identification of "sensitive" corporate areas, for each category of "predicate offence". Within each sensitive area, the so-called "sensitive" corporate activities were then identified, i.e. those activities for which the risk of the commission of the predicate offences set out in the Decree is most likely to occur, codifying, for each of these, different principles of conduct and control in relation to the specific risk of offence to be prevented, which must be complied with by all those who work there.

The Model is fully and effectively implemented in the Company's operations by connecting each sensitive area with the corporate structures concerned from time to time and with the dynamic management of processes and of the reference internal regulations, which must be based on the conduct and control principles spelled out for each such activity.

The approach adopted:

- helps make optimum use of the Company's store of knowledge concerning the internal policies, rules and regulations guiding and governing its decision-making and implementation concerning the prevention of unlawful acts, and, more in general, risk management and the performance of controls;
- makes it possible to manage the corporate operating rules with univocal criteria, including those relating to "sensitive" areas;

- facilitates the continual implementation and prompt alignment of processes and internal regulations with changes in the organisational structure and company operations, ensuring a considerable level of “dynamism” of the model.

Accordingly, the control of the risks under Legislative Decree No. 231/2001 by Neva SGR is ensured by:

- this document ("*Organisational, management and control model pursuant to Legislative Decree No. 231 of 8 June 2001*");
- the existing regulatory system, which is an integral and substantive part of this model.

The “Organisational, Management and Control Model” outlines in particular:

- the reference regulatory framework;
- the roles and responsibilities of the structures engaged in the adoption, effective implementation and modification of the model;
- the specific duties and responsibilities of the Surveillance Body;
- the information flows to and from the Surveillance Body;
- the system of sanctions;
- the training principles;
- the “sensitive” areas having regard to the types of offences identified in the Decree;
- the corporate activities at risk for the predicate offences (“sensitive” activities) and the rules of conduct and controls aimed at preventing such offences.

The Company's regulatory system, consisting of the "Governance Documents" (Articles of Association, Code of Ethics, Group Internal Code of Conduct, Regulations, Group Guidelines, Rules, etc.), Circulars, Organisational Manual, Functional Chart, Processes and other instruments, regulates at various levels the Company's operations in "sensitive" areas/activities and constitutes to all intents and purposes an integral part of the Model.

The regulatory framework is contained and catalogued, also with specific reference to "sensitive" activities, in a specific document repository, which is available via the corporate Intranet and constantly updated by the competent function in line with the development of operations.

Therefore, by matching the contents of the Model with the corporate regulatory framework it is possible to extract, for each of the “sensitive” activities, specific, precise and always up-to date Protocols that set out phases of activities, the structures concerned, control and conduct principles, and process operating rules and which make it possible to verify and streamline each activity phase.

Should the Asset Management Company extend its sphere of operations, it shall carry out a special assessment to identify any new sensitive areas and activities to be included in the Model with the related description of processes, control principles and principles of conduct.

2.5 The addressees of the Model

The Model and the provisions contained and referred to therein must be complied with by the company representatives and all Neva SGR personnel and, in particular, by those who perform sensitive activities.

Staff training and the dissemination of information on Model contents within the organisation are continuously ensured by the procedures described in detail in Chapter 6 below.

In order to ensure the effective and efficient prevention of offences, the Model is also addressed to external stakeholders (meaning self-employed or "para-subordinate" workers, professionals, consultants, agents, suppliers, business partners) who, by virtue of contractual relations, collaborate with the Company in the performance of its activities. Their compliance with the Model is ensured by a contractual clause – under penalty of termination – whereby they undertake to comply with the principles of the Model and the Anti-Corruption Guidelines and to report to the Surveillance Body and the Corporate Anti-Corruption Officer any offences or violations of the Model. The violation of obligations or other offences that may be committed during or in relation to their duties will to all intents and purposes constitute a serious violation within the meaning of Article 1455 civil code for the purposes of termination of the contract.

2.6 Model adoption, effective implementation and modification – Roles and responsibilities

In accordance with Article 6, paragraph I, point a) of the Decree, the “Model” is adopted by resolution of the Board of Directors, which also supervises its implementation, upon receiving the opinion of the Surveillance Body.

The Chief Executive Officer defines, also in their role as Employer pursuant to Legislative Decree No. 81/2008 and as Environmental Affairs Officer pursuant to Legislative Decree No. 152/2006, the structure of the Model to be submitted to the Board of Directors for approval with the support, for the areas of their respective competences, of the Functions within the company or outsourced within the Group, as well as the Internal Auditing Function.

Effective implementation and modification of the Model

The Board of Directors (or the entity formally delegated by it) is tasked with effectively implementing the Model, by assessing and approving the actions required to implement or amend it. In identifying such actions, the Board of Directors is assisted by the Surveillance Body.

The Board of Directors delegates the individual structures to implement Model contents and to regularly update and implement the internal regulations and corporate processes, which

are an integral part of the Model, in compliance with the control and conduct principles defined for each sensitive activity.

Effective and concrete Model implementation is also ensured:

- by the Surveillance Body, in the exercise of its powers of initiative and control over the activities carried out by the individual Corporate Functions in the sensitive areas;
- by the heads of the various Corporate Functions of the Company or of the relevant functions of the Intesa Sanpaolo outsourcer in relation to the risk activities carried out by them.

The Board of Directors, also with the help of the Surveillance Body, must also ensure updating of the sensitive areas and of the Model, in view of any adaptations that may be necessary.

Specific roles and responsibilities relating to Model management are also assigned to the structures indicated below.

Internal Auditing Function

In general, the Internal Auditing Function (outsourced by Intesa Sanpaolo) delivers ongoing and independent surveillance on the regular performance of operations and processes, in order to prevent or detect any anomalous or risky behaviour or situation. It assesses the efficiency of the overall internal control system and its ability to guarantee effective and efficient company processes.

This Function supports the Surveillance Body in monitoring compliance with and adequacy of the rules contained in the Model. Whenever problems are identified, it refers them to the competent functions for the appropriate mitigation actions.

Compliance and AML Function

The Compliance and AML Function ensures, over time, that effective rules, procedures and operational practices are in place to prevent breaches or violations of applicable provisions. It also provides assistance and advice to the other corporate structures for the pursuit of the purposes set out in the Decree.

With specific reference to the administrative liability risks introduced by the Decree, the Compliance and AML Function supports the Surveillance Body in carrying out its control activities by means of:

- defining and updating the Model, with the support of the Planning, Control Outsourcing and Operational Coordination Function, in accordance with the development of the reference legislation and changes in the corporate organisational structure, the Employer pursuant to Legislative Decree No. 81/2008 and the Environmental Affairs Officer pursuant to Legislative Decree No. 152/2006, to the extent of their competence;

- monitoring, over time, Model effectiveness with reference to the rules and principles of conduct for the prevention of sensitive offences; to this end the Function:
  - provides for the prior concurrence of internal operating procedures pertaining to sensitive areas pursuant to Legislative Decree No. 231/2001, prior to their issuance, in order to assess the correct application of the control and conduct principles provided for by the Model; it also proceeds, with a risk-based approach, to carry out specific assurance activities aimed at assessing the compliance of processes with the "protocols" provided for by the Model;
  - analyses the results of the Internal Corporate Functions' self-assessment process and statement on compliance with the control and conduct principles set out in the Mode[1]l;
- the examination of the results of the activities carried out by the Internal Auditing Function concerning the critical issues found during its audit activities.

The activities of the "Anti-Money Laundering Function" are also assigned to the Compliance and AML Function. It therefore continuously verifies that the company's procedures are consistent with the objective of preventing and countering the violation of external regulatory requirements (laws and regulations) and self-regulation on money laundering, terrorist financing, violation of embargoes and weapons and anti-corruption legislation.

To pursue the aims set out in the Decree, the Function, exclusively with regard to managing risks inherent to anti-money laundering, terrorism financing, embargoes and weapons and anti-corruption legislation:

- contributes to the definition of the Model's structure and to its update;
- promotes organisational and procedural amendments aimed at ensuring an adequate monitoring of the risks inherent to money laundering and terrorism financing;
- receives and forwards the periodic reports and information flows provided for in the "Guidelines for contrasting money laundering and terrorist financing and managing embargoes", including those addressed to the Anti-Money Laundering officer[2] if already appointed[3];
- ensures, in liaison with the Planning, Outsourcing Control and Operational Coordination Function and the Intesa Sanpaolo outsourcer for training-related activities, the preparation of appropriate training activities, aimed at keeping employees and collaborators constantly updated.

Intesa Sanpaolo - Outsourcer for Corporate Secretariat activities

[1] Declarations relating to activities outsourced to Intesa Sanpaolo are not required as they follow the similar procedure in the Parent Company.

[2] Figure introduced pursuant to the Bank of Italy's Provisions dated 1 August 2023

[3] Neva SGR will appoint the Anti-Money Laundering Officer within the terms provided for by the Bank of Italy Provision of 1 August 2023

The outsourcer provides assistance with specific reference to the activities of the Surveillance Body, including the drafting of its minutes.

Planning, Outsourcing Control and Operational Coordination Function

The Planning, Outsourcing Control and Operational Coordination Function, in order to better oversee the consistency of the organisational structure and governance mechanisms with respect to the objectives pursued with the Model, is responsible for the following activities:

- Support the competent bodies in the preparation of the financial statements and management reports of the managed funds;
- prepare the budget and carry out management control activities;
- oversee expense management;
- act as contact for non-investment contracts;
- act as contact for outsourced activities, monitoring and control of service contracts;
- prepare proposals for setting up the organisational structure, defining its missions, organisation charts and functions, in order to submit it for approval to the Chief Executive Officer and, in the cases provided for, to the Board of Directors;
- propose to the Chief Executive Officer the rules for the design, formalisation and management of organisational processes, and coordinate the issuing and collection of company rules and procedures;
- support the design of the organisational processes or validate procedures prepared by other structures, ensuring their consistency with the overall organisational plan;
- cooperate with the Compliance and AML Function, with the Employer pursuant to Legislative Decree No. 81/2008, with the Environmental Affairs Officer pursuant to Legislative Decree No. 152/2006, with the Internal Auditing Function and the other structures concerned, each within its sphere of competence, in updating the regulatory system and the Model (following changes to the applicable legislation or in the company's organisational setup and/or operating procedures, relevant for the purpose of the Decree);
- disseminate the internal rules throughout the Company's organisation through the company's Intranet.

Intesa Sanpaolo - Outsourcer for Human Resources activities

- scheduling training plans and awareness-raising actions aimed at all employees on the importance of conduct in compliance with corporate rules, on understanding the contents of the Model, the Internal Code of Conduct, Code of Ethics and Anti-Corruption Guidelines of the Group, and specific courses addressed to the staff operating in the

sensitive areas, in order to clarify in detail issues, early warning signs of anomalies or irregularities and the mitigation actions to be taken for anomalous or risk-exposed operations;

- monitoring, with the support of Internal Auditing, the sanctioning process in the event of the detection of violations of the Model, supporting the competent Bodies in defining and disbursing the relevant sanctions. In this regard, either directly or through the Internal Auditing Function, the structure provides all information on facts and conduct to the Surveillance Body, which analyses it in order to prevent future violations, as well as to monitor the adequacy of the Model.

Corporate Functions

The Corporate Functions are tasked with the execution, proper functioning and sustained effective process application over time.

For the specific purposes of the Decree, the Corporate Functions have a duty to:

- review – in the light of the rules of conduct and principles applicable to sensitive activities – the practices and processes falling under their remit, to make them suitable to prevent unlawful conduct;
- report to the Surveillance Body any cases of irregularities or anomalous conduct.

In particular, the above-mentioned Corporate Functions in the performance of sensitive activities should pay the highest and constant care in verifying the existence of and remedying any shortcomings in the regulations or procedures which may give rise to foreseeable risks of “predicate offences” being committed within the activities under their remit.

Employer and Principal pursuant to Legislative Decree No. 81/2008, Environmental Affairs Officer pursuant to Legislative Decree No. 152/2006

The parties identified as Employer and Principal pursuant to Legislative Decree No. 81/2008, and Environmental Affairs Officer pursuant to Legislative Decree No. 152/2006, only as concerns their respective area of responsibility for managing the risks relating to the environment, workplace health and safety at temporary or mobile construction sites and in environmental matters shall:

- identify and assess the emergence of risk factors for predicate offences;
- issue operational and organisational provisions so as to fully meet the obligations concerning the protection of occupational health and safety as well as environmental protection.
- participate in defining the Model’s structure and in updating it.

The activities in question are carried out with the support of the competent Parent Company structures in accordance with the provisions of the service agreements contracted between the parties from time to time.

2.7 Outsourced activities

Neva's organisational model envisages the outsourcing (hereinafter also “outsourcing”) of business activities, or parts thereof, to the parent company and/or third-party suppliers, also external to the Group.

In particular, the Company has entered into agreements for the performance of certain activities with the Parent Company in the following areas:

- Internal Auditing;
- Human Resources: management and administration of executives and continuing coordinated collaborations, personnel administration (non-executive), industrial relations, personnel services, consulting on legal and contractual regulations, labour disputes, disciplinary proceedings, managerial initiatives, community development, evaluation systems, labour regulations, welfare and mobility services, recruitment and internships - administrative activities, mobility administration, personnel management, intra-group mobility, international mobility and compensation support, global banding;
- Safety at work, environment and energy consultancy on Legislative Decree No. 81/2008 (including covering the role of Manager of the Prevention and Protection Department, activities relating to the prevention and protection service and health surveillance), safety at work and environmental protection;
- Collective Bodies and Corporate Affairs: compulsory fulfilments related to corporate bodies, activities related to corporate meetings and activities related to boards;
- Institutional Affairs And External Communication: consultancy and management relating to institutional communications, images, brands, websites, official publications, sponsorships and giveaways; event organisation, consultancy and purchase of advertising space, management and development of marketing communications and media relations management;
- Privacy: privacy consulting and compliance, privacy compliance monitoring,
- Legal and litigation: legal advice and assistance, judicial and out of court dispute management;
- Group treasury and finance: access to ST money markets in euro and other currencies;
- Cybersecurity and Business Continuity Management;
- Risk Management: Operational, Reputational, IT & cyber risk;
- Organisation and general services;

- Development and Learning policies: training design and delivery, remuneration policies;
- Real estate and logistics: technical property management and integrated logistics;
- Purchasing: insurance management and sourcing;
- Information systems: integrated application management, email and file sharing, desktop management, multifunctional printers, MDM Mobile Device Management, fixed and mobile telephony, data network and multimedia services;
- Internal communication: internal publishing and intranet;
- Cost management: infoprovider;
- Operations: help desk;
- Physical security management.

In addition, the Company has entered into specific outsourcing contracts with suppliers outside the Intesa Sanpaolo Group to perform the following activities:

- the administrative and accounting services of the Asset Management Company and the managed Funds and the Business Information System (entrusted to PREVINET SpA, a company specialised in providing administrative services and IT solutions for supplementary welfare, insurance and finance operators).
- the asset valuation function of the managed funds (entrusted to PWC ADVISORY S.p.A.).

Outsourcing of the activities is carried out in accordance with the prescriptions of the Supervisory authorities and is formalised through the conclusion of specific contracts that enable Neva SGR to:

- take all decisions by exercising its autonomy, as it maintains the necessary competences and responsibilities on the activities relating to the outsourced services;
- consequently maintain guidance and control powers on the outsourced activities.

In particular, these contracts envisage, in compliance with current legislation on outsourcing, specific contractual clauses including:

- the outsourced activities in detail;
- the procedures for providing the services;
- the specific service levels;
- the verification and control powers remaining with Neva SGR;
- the procedures for setting rates for the services provided;
- suitable reporting systems;
- appropriate safeguards protecting the Asset Management Company’s information assets;

- the obligation of the outsourcer to operate in compliance with applicable laws and regulations, and to ensure that third parties appointed to carry out outsourced activities observe said laws and regulations;
- the possibility for Neva SGR to terminate the contract in the event the outsourcer violates: (i) the laws and directives from the Supervisory Authorities that may result in penalties imposed on the principal; (ii) the obligation to implement activities in compliance with the principles laid down in the Organisational, Management and Control Model pursuant to Legislative Decree No. 231 of 8 June 2001 adopted by Neva SGR and with the Group's Code of Ethics, Internal Code of Conduct, and Anti-corruption Guidelines.

The Asset Management Company's Planning, Outsourcing Control and Operational Coordination Function verifies on an ongoing basis, also through control of the required service levels, compliance with contractual clauses, hence adequacy of the activities performed by the service provider.

2.8 The role of the Parent Company

Without prejudice to the autonomous responsibility of each Intesa Sanpaolo Group Company for the adoption and effective implementation of its own Model pursuant to the Decree, Intesa Sanpaolo, in exercising its specific function as Parent Company, the Bank has the power to establish criteria and guidelines of a general nature and to verify, through the Compliance, Internal Auditing and M&A and Group Investments functions, whether the Models of Group companies comply with such criteria and guidelines.

2.8.1 Group guidelines concerning the Administrative Liability of Entities

In order to harmonise at Group level the procedures for transposing and implementing the contents of the Decree by putting in place appropriate risk control procedures, we outline below the guidance principles defined by the Parent Company, which all the companies incorporated in Italy and therefore also Neva, are required to comply with, in accordance with their legal autonomy and with the principles of sound corporate management.

In particular, each company concerned shall:

- adopt its own Model, after identifying the corporate activities at risk for the offences provided for by the Decree and the measures best able to prevent such offences. In preparing the Model, the Company shall follow the principles and contents of the Parent Company's Model, except where there are specific situations relating to the nature, size or type activity pursued or the company's structure, the organisation and/or the allocation of internal delegations making it necessary or advisable to adopt different

measures in order to pursue the Model's objectives more effectively, while always respecting the above-mentioned principles and those laid down in the Code of Ethics and in the Internal Code of Conduct and Anti-corruption Guidelines of the Group.

In the case of substantial discrepancies with the principles and contents of the Model of Parent Company, the Parent Company's Compliance function shall be informed of the reasons for such differences, and shall receive the final draft of the Model prior to its approval by the Corporate Governance Bodies.

The Company shall inform the Compliance function of having adopted the Model by sending a copy thereof and the Board of Directors' approval resolution. Pending approval of the Model, the Company shall adopt all appropriate means to prevent unlawful conduct;

- promptly appoint the Surveillance Body, in line with the Parent Company's recommendations on the persons to be appointed. The Compliance, M&A and Investments functions of Intesa Sanpaolo S.p.A. are informed of the nomination. If the members of the Surveillance Body are not the same as those of the subsidiary's control body, the Management Control Committee of Intesa Sanpaolo SpA must be provided with specific information in the report on activities overseen by the Surveillance Body;
- ensure systematic Model updating as required by legislative and organisational changes, or where significant and/or repeated breaches of the rules of the Model make it necessary. Any legislative amendments shall be notified by a specific communication to be sent to the Company by the Parent Company's Compliance function. Confirmation of the Model having been updated shall be provided to the Compliance function following the procedures described above;
- prepare – in coordination with the Parent Company's Human Resources and Compliance functions and with the support of the Training and Internal Communication functions – training and communication activities addressed indiscriminately to all personnel, as well as specific training interventions aimed at figures engaged in activities that are more "sensitive" under the Decree, – including any representatives shared with the Parent Company – with the aim of creating widespread knowledge and an adequate corporate culture on the subject;
- adopt appropriate controls of the processes which are "sensitive" with respect to the Decree, covering their identification, documentation and publication within the corporate regulatory system. In addition, sensitive processes must be identified annually by the company's compliance function or, if not present, by the function specifically identified to monitor the administrative liability of entities with a risk-based approach, those deemed to have a higher degree of risk, on the basis of both qualitative considerations with

respect to the predicate offences and the existence or otherwise of specific safeguards to mitigate the relevant risk. For these processes, the Company's Compliance Function provides for:

  - the issuance of a prior concurrence on internal operating procedures, prior to their issuance, in order to assess the correct application of the control and conduct principles laid down in the Model and the compliance of processes with the “protocols” set out in the Model;
  - the performance of specific assurance activities, with a risk-based approach, aimed at assessing the compliance of processes with the “protocols" laid down in the Model.

- performs, once a year, a self-assessment review of the activities carried out to verify the degree of Model implementation, with special regard to compliance with control and conduct principles and with operating rules. The self-assessment review shall be initiated in coordination with the Parent Company’s Risk Management and Compliance functions;
- the Parent Company Compliance function to receive a copy of periodic reports, including the results of the self-diagnostic process, presented by the Compliance and AML function to the Surveillance Body.

The Surveillance Body of the Company also transmits to the Parent Company's Management Control Committee and to the Surveillance Body of the Parent Company, through the outsourcer of ISP Management Service Subsidiaries, the periodic report, usually every six months, on the activities carried out submitted to the Board of Directors, together with any observations of the Board itself.

Information flows can also be provided between the Surveillance Body of the Parent Company and the Bodies of the companies - also through training meetings on topics of common interest - in order to enable the coordination of the Group's Surveillance Bodies and a better and more effective supervision of preventive measures within the individual corporate entities.

With regard to the above-mentioned activities, the competent Parent Company functions shall, within their respective spheres of competence, support and assist the companies in performing their duties.

3 THE SURVEILLANCE BODY (SB)

3.1 Composition and duties of the Surveillance Body

The task of continuously monitoring effective implementation of the Model, ensuring observance and proposing updates to improve the efficacy of crime and unlawful acts prevention pursuant to Article 6 of Legislative Decree No. 231/2001, which is entrusted to the Surveillance Body, a body within the Entity with autonomous powers of initiative and control.

The functions of the Surveillance Body are assigned to the Board of Statutory Auditors for the entire period in which it remains in office and in the composition determined from time to time in application of the rules of replacement, supplementation, suspension and disqualification of its members pertaining to the Body.

The Surveillance Body routinely avails itself of the structures of the Company and of the Parent Company to perform its supervisory and control tasks and, first and foremost, of the Internal Auditing function, a structure institutionally endowed with technical skills and resources, both human and operational, suitable to guarantee the performance on an ongoing basis of the audits, analyses and other necessary tasks. The Internal Auditing function attends all meetings of the Body.

3.2 Autonomy of the Body

The Surveillance Body has powers of initiative and control over the activities of the Company. It is not vested with management powers.

In order to allow it to exercise its functions with complete independence, the Surveillance Body is attributed its own annual budget, which is approved by the Board of Directors, upon the favourable opinion of the Body itself.

In order to ensure that the powers of initiative and control are exercised autonomously towards all persons who are subject to the rules which are set forth or referred to in the Model, the Surveillance Board may exceed the budget set and approved by the Board of Directors pursuant to the preceding paragraph in exceptional cases of urgency, without requiring prior authorisation. In such cases, the Body must appropriately justify in its minutes the expense and existence of the urgency requirements and obtain ratification by the Board of Directors at the latter’s next meeting.

The operation of the SB is governed by a Regulation of the activities and duties conferred upon it (determination of the frequency of its meetings and audits, convocation and meeting

procedures, identification of the criteria and procedures for analysis, appointment of the Chair).

3.3 Constitution, appointment, duration and remuneration of the Surveillance Body

3.3.1 Constitution and appointment

The Surveillance Body consists of three standing members and two alternate members; the latter take over only in the cases provided for by section 3.4.2 Grounds for replacement or disqualification.

The Shareholders' Meeting constitutes the Surveillance Body, appointing the three standing and two alternate members from among individuals external to the Company who fulfil the requirements specified under section 3.4.

3.3.2 Honour

The Chair of the Surveillance Body is the Chair of the Board of Auditors.

In the event of the revocation, disqualification or other cause of termination of one or more members, the alternate member shall automatically take over from the moment the Chair informs them of the declaration of suspension or temporary inability of the standing member and shall remain in office until the moment the Chair informs them of the end of the cause that led to the taking over.

Members appointed as alternates shall remain in office until expiration of the Surveillance Body's term, as indicated under paragraph 3.3.3.

3.3.3 Duration

The members of the Surveillance Body remain in office for the duration established by the Articles of Association for the members of the Board of Statutory Auditors; the standing members and alternate members of the Board of Statutory Auditors remain in office for three financial years and expire on the date of the Shareholders' Meeting called to approve the financial statements for the third financial year of their office.

3.3.4 Remuneration

The Board of Statutory Auditors performs the functions of the Surveillance Body for the entire period in which it remains in office and in the composition determined from time to time in application of the rules of replacement, supplementation, suspension and disqualification of its members proper to the body, without prejudice to those hypotheses, provided for in the following paragraphs, in which the Surveillance Body will have a different composition from that of the Board of Statutory Auditors. The remuneration due for the

performance of the functions of the Surveillance Body is established by the Shareholders' Meeting when appointing the Board of Statutory Auditors; it is determined taking into account the functions performed by the Statutory Auditors themselves as members of the Surveillance Body and is indicated separately from the remuneration due to the members as members of the Board of Statutory Auditors.

Standing and alternate members shall also receive reimbursement of documented expenses incurred for participation in the meetings.

3.4 Eligibility requirements, grounds for disqualification and suspension

3.4.1 Professionalism, honour and independence

Without prejudice to the requirements of professionalism, honour and independence provided for by the laws in force, in order to provide the Board of Statutory Auditors with additional skills for the best performance of the functions of the Surveillance Body assigned to it, at least one of the standing members must be chosen from among persons possessing specialised skills deriving for example from having carried out professional activities for at least three years in matters pertaining to the sector in which the Company operates and/or from having adequate knowledge of the organisation, control systems and main corporate processes, or from having been - or being - part of Surveillance Bodies.

In addition to the possession of the above-mentioned requirements, the standing members and alternate members must possess the following additional **requirements of honour**, according to which members of the Surveillance Body cannot include those who:

- have been convicted, by a sentence which has become irrevocable, even if the sentence is conditionally suspended, pursuant to Article 163 of the Italian Criminal Code, without prejudice to the effects of rehabilitation, for one of the offences among those for which Legislative Decree No. 231/2001 is applicable, or for the offences referred to in Royal Decree No. 267/1942 (bankruptcy law), or for tax offences. Conviction is also understood as a sentence pronounced pursuant to Article 444 of the Code of Criminal Procedure, without prejudice to the effects of the judicial declaration of extinction of the offence pursuant to Article 445, paragraph 2 of the Code of Criminal Procedure;
- have held the position of member of the Surveillance Body within companies or entities against which the sanctions provided for in Article 9 of the same Decree have been applied, with a final ruling (including the sentence issued pursuant to Article 63 of the Decree), for offences committed during their term of office;
- have been subject to the application of ancillary administrative sanctions resulting in the temporary loss of the eligibility requirements or the temporary disqualification from carrying out administration, management and control functions at intermediaries or

companies with listed shares, pursuant to Legislative Decree No. 58/1998 (Finance Consolidation Act) or Legislative Decree No. 385/1993 (Consolidated Banking Act);

Within thirty days of their appointment, the Surveillance Body verifies the existence of the requirements for its members and alternates, on the basis of a declaration made by the individuals concerned, and informs the Board of Directors of the outcome.

Dishonesty on the part of the member of the Body determines their immediate disqualification from this function.

3.4.2 Grounds for disqualification, suspension and temporary impediment

After their appointment, the Surveillance Body's standing and alternate members **shall lapse from office** where:

- they are liable to be struck off or disqualified from holding the office of statutory auditor, also as a consequence of the fact that they no longer meet the requirements and criteria of suitability for the office prescribed by law;
- it is ascertained that they have held the position of member of the Surveillance Body within a company or entity against which the sanctions provided for in Article 9 of the Decree, for offences committed during their term of office, have been applied with a final ruling (including a sentence issued pursuant to Article 63 of the Decree);
- it is ascertained that they have been convicted with a final sentence (where conviction is also understood as a sentence pursuant to Article 444 of the Italian Code of Criminal Procedure), even if the sentence is conditionally suspended pursuant to Article 163 of the Criminal Code, for one of the offences among those for which Legislative Decree No. 231/2001 is applicable, or for the offences referred to in Royal Decree No. 267/1942, or for tax offences;
- they are subject to the definitive application of ancillary administrative sanctions resulting in the temporary loss of the eligibility requirements or the temporary disqualification from carrying out administrative, management and control functions at intermediaries or companies with listed shares, pursuant to Legislative Decree No. 58/1998 or Legislative Decree No. 385/1993.

The members of the Surveillance Body must notify the Chair of the Board of Directors, under their full responsibility, of the occurrence of any of the above-mentioned grounds for disqualification.

The Chair of the Board of Directors, also in all further cases in which he has direct knowledge of the occurrence of a cause for disqualification, without prejudice to any measures to be taken pursuant to the law and the Articles of Association in relation to the office of statutory auditor, shall promptly convene the Board of Directors so that it may proceed – at its first meeting following the occurrence of such knowledge – to declare the

disqualification of the person concerned from the office of member of the Surveillance Body. At the same time – and provided that the forfeiture of office does not depend on the termination of the statutory auditor's office as well, in which case the statutory rules for the integration of the body would apply – the Board of Directors shall replace them with the eldest alternate auditor. In the event of the lapse of an alternate auditor, in the absence of replacement measures by the Shareholders' Meeting and in any case until such measures are issued, the Board of Directors shall provide for the replacement.

In addition to those **grounds for suspension** from the office of member of the Surveillance Body, which, pursuant to the legislation in force, lead to suspension from the office of Statutory Auditor, the following further grounds are also set out below:

- a conviction, even if not final, of the member of the Surveillance Body or other sentences would result in suspension from the Board of Directors pursuant to applicable laws;
- cases in which after being appointed, members of the Board of Directors are found to have carried out the same role within a company which has received, by non-final measure, the sanctions laid down in Article 9 of the Decree, concerning unlawful acts committed during their term of office;
- a non-definitive conviction, to which the sentence handed down pursuant to Article 444 of the Code of Criminal Procedure is equivalent, even if the sentence is suspended, for one of the following offences under Legislative Decree No. 231/2001; offences relating to business crisis and insolvency[4]; tax offences;
- committal for trial for one of the offences mentioned in the above paragraph;
- an illness or accident or other justified impediment that continues for over three months, hindering the member of the Surveillance Body from participating therein. In the case of illness, accident or justified impediment of a standing member referred to in this point, the alternate member takes over after three months, exercising the functions related to the position of member of the SB for no more than one quarter, after which the Chair of the Board of Directors proceeds according to the terms indicated above.

The members of the Surveillance Body must notify the Chair of the Board of Directors, under their full responsibility, of the occurrence of any of the above-mentioned grounds for suspension.

In any case, should the Chair of the Board of Directors become aware of the occurrence of one of the aforementioned grounds for suspension, without prejudice to any measures to be taken pursuant to the law and the Articles of Association in relation to the position of Statutory Auditor, they shall promptly convene the Board of Directors so that it may declare,

[4] The reference is to the offences in Royal Decree 267/1942 and the offences in the Code of business crisis and insolvency (Legislative Decree No. 14/2019) whose entry into force has been postponed to 1 September 2021.

at its first subsequent meeting, the suspension of the person, in respect of whom one of the aforementioned grounds has occurred, from the position of member of the Surveillance Body. In that case, the oldest alternate auditor takes over ad interim.

Unless otherwise provided for by law and regulations, the suspension may not last longer than six months, after which the Chair of the Board of Directors shall enter the possible revocation among the items to be addressed in the next Board meeting. The non-revoked member is reinstated in full.

If the suspension concerns the Chair of the Surveillance Body, the chair role shall be assumed, for the duration of the suspension, by the most senior member by appointment or, in the event of equal seniority, by the most senior member by age.

In the event that causes arise which **temporarily prevent** a standing member of the Surveillance Body from performing their functions or from performing them with the necessary independence and autonomy of judgement, they shall declare the existence of the legitimate impediment and, if it is due to a potential conflict of interest, the cause from which it arises; they shall also refrain from taking part in the meetings of the Body itself or in the specific resolution to which the conflict refers, until such time as the said impediment persists or is removed.

Sickness or injury or other justified impediment lasting more than three months and preventing attendance at meetings of the Body shall also constitute grounds for temporary impediment.

In the event of a temporary impediment, the eldest alternate auditor automatically takes over. The alternate member ceases to hold office when the reason for taking over ceases to exist.

This is without prejudice to the right of the Board of Directors, when the impediment continues for a period of more than six months, extendable by a further six months on no more than two occasions, to remove the member for whom the aforesaid grounds for impediment have arisen and to replace them with another standing member.

3.5 Duties of the Surveillance Body

The Surveillance Body, in pursuit of its ordinary activity shall oversee:

i) the efficiency, effectiveness and adequacy of the Model and the provisions contained therein insofar as preventing the offences covered by Legislative Decree No. 231/2001;

ii) compliance with the provisions of the Model and the provisions referred to therein by its addressees, assessing the consistency of actual behaviour with the Model and any discrepancy, through information flow analyses and reports to be submitted by the heads of the various corporate functions;

iii) updating of the Model when necessary, as a consequence of confirmed and significant breaches of the provisions of the Model, significant changes in the Company's organisational set-up and procedures, or of the adoption of new legislation in this area, submitting proposals to the competent Corporate Bodies regarding appropriate modifications or integrations;

iv) compliance with the principle and values set forth in the Intesa San Paolo Group's Code of Ethics;

v) the existence and effectiveness of the company's prevention and protections system with regard to occupational health and safety;

vi) the implementation of Personnel training activities see section 6.2 below;

vii) the adequacy of the procedures and channels for internal reporting of unlawful conducts pursuant to Legislative Decree No. 231/2001, or any non-compliance with the Model and their suitability in guaranteeing the confidentiality of the person making said reports within the reporting management system;

viii) respect of the ban on retaliatory or discriminatory actions, whether direct or indirect, against the whistleblower for reasons directly or indirectly related to the whistleblowing;

ix) the initiation and implementation of the procedure for imposing disciplinary sanctions, by the competent functions, where infringements of the Model are found.

The Surveillance Body shall also monitor, within the scope of its functions and duties, compliance with the provisions relating to prevention of the use of the financial system for the purpose of money laundering and the financing of terrorism laid down in Legislative Decree No. 231/2007.

Pursuant to the aforementioned prerogatives of autonomy and independence of the Surveillance Body, the functioning and observance of the Model are also ensured through constant monitoring, planning, programming and exchange of information flows with corporate bodies and functions.

The Surveillance Body has as its direct contacts and interlocutors, in the performance of its supervisory and control tasks, the heads of the Internal Auditing and Compliance functions (hereinafter: "Surveillance Body Contacts").

The Surveillance Body contacts shall provide, each within his/her purview, adequate support, assistance in the investigations and information to the Body, providing to it all the resources required for such activities, without being required to coordinate among themselves internally, except if the concurrent intervention of all the contacts has been requested.

The relation between the contacts, as well as the personnel they appoint and make available for the specific discovery and investigation requirements, and the Body is fundamental for the optimal performance of the tasks which the Body is specifically assigned and are not of a hierarchical character, notwithstanding the autonomy of the Body's powers of control and its non-involvement in management functions. Indeed, there is no change to the attributions, powers and organisational reporting and functional lines of the Surveillance Board contacts as provided by the Company's internal organisation and the applicable laws.

The contacts of the Surveillance Body are required to immediately transmit to it all the information acquired by them which are relevant to the Model, in terms of control and monitoring.

When the Body requests the execution of a specific assessment, the involved contacts and the individuals assigned by the latter, are required to maintain the contents of the request they received and the specifically requested investigation activity strictly confidential, except as required by applicable laws. In any case with regard to the outcomes of specifically requested investigation activities, the contacts shall inform the Body of any events or critical issues that render observance of disclosure and reporting obligations necessary pursuant to applicable laws and the Company's internal regulations.

In order to monitor the specialised regulatory areas, the Surveillance Body shall also enlist the assistance of all functionally competent structures and corporate roles that have been established pursuant to specific sector regulations (Employer, Manager of the Prevention and Protection Department, Employee Safety Representative, Competent Doctor, Anti-Money Laundering function Manager, Head of Suspicious Activity Reporting, Environmental Affairs Officer pursuant to Legislative Decree No. 152/2006).

When required due to the need for specialisations which are not available or as appropriate, the Surveillance Body shall enlist the assistance of external consultants to whom it shall delegate technical operations, investigations and the verifications required for conducting its controls.

The Surveillance Body, either directly or through the various designated corporate structures, has access to all the activities carried out by the Company and the outsourcers in the areas at risk and to the relevant documentation, both at the Company's headquarters and at the peripheral structures of the Company and the outsourcers.

In order to provide the Surveillance Body with an overview of the planning of second-level (compliance and anti-money laundering) and third-level (internal audit) control activities, the

functions concerned make available to the Surveillance Body their plans on the control activities planned in the sensitive areas of the Model.

Based on these documents the Surveillance Body assesses the adequacy of the audit plans on the individual sensitive corporate activities and carries out any further action to strengthen the control plans proposed by the individual structures concerned.

The control activity which is set up and organised by internal structures is based on specific protocols designed and regularly updated based on the results of the risk analysis (i.e. the ongoing process of prior identification, classification and assessment of the risks, whether internal or external), and of the internal controls, from which the plans for audit activities are derived.

These activity plans also take into account any remarks and suggestions received in various capacities from the Corporate Bodies.

The Control Functions shall periodically report to the Surveillance Body on this activity.

If considered necessary or advantageous, the Surveillance Body may exchange information with the independent auditors.

For issues that fall under the Board of Directors' remit, the Body may request the Chair of the Board – and, in particularly significant cases, the Chief Executive Officer – for specific information on issues which it considers appropriate to examine in order to better conduct its duties of monitoring the operation, efficacy and observance of the Model.

3.6 Procedures and frequency for reporting to the Corporate Bodies

The Surveillance Body in all circumstances in which it considers it necessary or appropriate, or if requested, reports to the Board of Directors on the operation of the Model and the fulfilment of the obligations laid down in the Decree.

At least once every six months, the Surveillance Body shall submit to the Board of Directors a specific report on the adequacy of and compliance with the Model, which shall refer to:

- the activity carried out;
- the results of the activity carried out;
- the planned corrective and improvement actions and their progress.

After the examination by the Board of Directors, the Surveillance Body shall forward the report – accompanied by any remarks made by the Board of Directors – to the Parent Company's Management Control Committee, through the Intesa Sanpaolo S.p.A. Collective Bodies and Corporate Affairs Head Office.

4 INFORMATION FLOWS TO THE SURVEILLANCE BODY

4.1 Information flows in the case of particular events

The Surveillance Body must be informed, by means of information provided by the Employees, the Heads of the Corporate Functions, the Corporate Bodies, the external parties (meaning suppliers, agents, consultants, independent professionals, self-employed or "para-subordinate" workers, commercial partners) about any events which may give rise to liability for Neva SGR pursuant to the Decree. In particular, any detailed information based on precise and consistent evidence must be reported without delay, concerning:

- the commission, or suspected commission, of offences provided for in Legislative Decree No. 231/2001;
- the violations of the rules of conduct or procedures contained in this Model and in the internal rules referred to therein;
- initiation of judicial proceedings against recipients of the Model for offences provided for by Legislative Decree No. 231/2001.

Such events can be reported: through the Head of the pertaining structure directly to the Surveillance Body or via the Internal Auditing Function, which after duly investigating the matter, informs the Surveillance Body of any reports received and provides a statement of any related facts discovered.

The external parties shall submit their reports directly to the Surveillance Body.

The Surveillance Body assesses information received and adopts measures under its responsibility and at its discretion, consulting the whistleblower and/or person responsible for the alleged infringement and justifying any decision not to proceed with an internal investigation in writing.

In addition to the reports on the above-mentioned breaches, the following information shall be submitted to the Surveillance Body on a mandatory basis and immediately:

- via the Internal Auditing function, any information concerning: the measures and/or information issued by judicial police bodies or any other authority, without prejudice for the secrecy obligations laid down in the law, indicating that investigations are in progress, also against unknown persons, for offences falling within the scope of Legislative Decree No. 231/2001, if such investigations concern the Company or its Employees or Corporate bodies or in any case involve the Company's liability;
- through the Internal Auditing Function, regarding facts, acts, events or omissions indicating the risk of infringement of the rules of the Decree, observed by the corporate control functions as part of their activity and the relative mitigation actions.

Each company structure given a specific role in a phase of a sensitive process must promptly notify the Surveillance Body of its conduct that significantly differs from the conduct described in the process, and the reasons making this deviation necessary or appropriate.

In the case of events which might give rise to serious liability for Neva SGR, the Internal Auditing Function, acting in accordance with Legislative Decree No. 231/2001, shall promptly inform the Chair of the Surveillance Body and shall prepare a specific report describing in detail the event, the risk, the staff involved, the disciplinary measures adopted and the solutions put in place to avoid recurrence of the event.

4.2 Internal reporting systems

In addition to the ordinary procedure provided for in the preceding paragraph, reports concerning:

- the commission, or suspected commission, of offences provided for in Legislative Decree No. 231/2001;
- the violations of the rules of conduct or procedures contained in this Model and in the internal rules referred to therein;

may be carried out by the persons referred to in paragraph 4.1 and by the shareholders also directly:

- to the Surveillance Body, at the addresses "Neva SGR S.p.A. - Surveillance Body, Corso di Castelfidardo, 22 - 10128 Turin", or "*odv@nevasgr.com*";
- through the specific reporting channels set up by the Company in accordance with Legislative Decree No. 24/2023[5] and with the provisions governing specific sectors (Consolidated Banking Act, Finance Consolidation Act, anti-money laundering legislation, etc.) and governed by the "Group Rules on internal systems for reporting violations (whistleblowing)" [6], to which reference should be made for the operational aspects (identification of channels, persons who may report[7]).

[5] Legislative Decree No. 24/2023, issued in implementation of Directive (EU) 2019/1937, comprehensively regulated the subject of reporting systems and in particular amended Legislative Decree No. 231/2001 by replacing paragraphs 2-bis, 2-ter and 2-quater of Article 6, which governed those systems, with a new paragraph 2-bis, which provides that the organisation and management models must provide for internal reporting channels, the prohibition of retaliation and the disciplinary system pursuant to Legislative Decree No. 24/2023, de facto referring to the latter for the relevant discipline.

[6]] The references of internal channels are published both on the corporate intranet and on the Group's website in the dedicated sections

[7] According to the provisions of Legislative Decree No. 24/2023, reports may be made by: employees and self-employed workers who perform or have performed their work activities at the Group, holders of a professional collaboration relationship pursuant to Article 409 of the Italian Code of Civil Procedure (e.g. agency relationship) and Article 2 of Legislative Decree No. 81/15 (collaborations organised by the principal), workers or collaborators who supply goods or services or perform works for third parties and who perform or have performed their work for the Group, freelancers and consultants who perform or have performed their work for the Group, volunteers and trainees (paid and unpaid), shareholders (natural persons), persons with administrative, control, supervisory or representative functions.

The reports thus received, processed in accordance with the procedures and deadlines laid down in Legislative Decree No. 24/2023, after initial examination, are sent to the competent function - identified on the basis of the specific case - for the purposes of initiating the necessary investigations and subsequent reporting to the Surveillance Body[8].

4.3 Protection measures and prohibition of retaliation

Neva SGR guarantees whistleblowers[9], regardless of the channel used, from any form of retaliation, discrimination or penalty and in any case ensures the utmost confidentiality regarding their identity, without prejudice to legal obligations. These measures are also extended to connected persons (e.g. relatives of the whistleblower who have working relations with the company and "facilitators").

The disciplinary system provided for in the Decree, in the implementation of which the sanctions set out in Chapter 5 below are established, also applies to those who:

- violate the obligations of confidentiality concerning the identity of the whistleblower or the prohibition of discriminatory or retaliatory acts;
- report, with malice or gross negligence, facts that turn out to be unfounded.

4.4 Periodic information flows

The Surveillance Body also exercises its control responsibilities through the analysis of systematic periodic information flows transmitted by the functions performing first-level control activities (Company Functions), the Compliance and AML Function, the Internal Auditing Function, the Planning, Control Outsourcing and Operational Coordination Function, the Employer pursuant to Legislative Decree No. 81/2008 and the Environmental Affairs Officer.

4.4.1 Information flows from Corporate Functions

Once a year, the heads of the Corporate Functions involved in the performance of “sensitive” activities within the meaning of Legislative Decree No. 231/2001 shall perform a self-assessment review of the activities carried out to verify the degree of Model

[8]] For the reports addressed directly to the Surveillance Body: (i) the first examination is aimed at assessing their relevance for the purposes of Legislative Decree No. 231/2001 and is conducted by the Surveillance Body with the support, where necessary, of the competent functions of the Company; (ii) reporting only concerns reports found to be material. For the procedures for the management and reporting of the reports received through the specific channels set up by the Company pursuant to Legislative Decree No. 24/2023, reference should be made to the provisions of the aforementioned "Group Rules on Internal Violation Reporting Systems (whistleblowing)”

[9] Pursuant to Legislative Decree No. 24/2023, protections are also granted to the following persons: (i) facilitators (the persons who assist the whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential), (ii) persons in the same work context as the whistleblower and who are linked to them by a stable affective or kinship relationship up to the fourth degree, (iii) co-workers of the whistleblower who work in the same employment context and who have a regular and current relationship with this person, (iv) entities owned by or for which the whistleblower works, as well as entities operating in the same employment context as the whistleblower.

implementation, with special regard to compliance with control and conduct principles and with operating rules.

Through this formal self-assessment exercise, they highlight any problem areas in the processes they operate, any departures from the guidelines set out in the Model or in general from the regulatory framework, and the adequacy of such regulations, and shall highlight the actions and initiatives adopted or planned to address such problems.

The Corporate Functions' assessments shall be sent once a year to the Compliance and AML Function, which shall file these reports, keeping them available for the Surveillance Body to which it shall forward a report setting out the results.

The method for implementing the self-assessment exercise, which falls under the Company's broader Operational Risk Management process, follows the guidelines and tools made available by Intesa Sanpaolo.

4.4.2 Information flows from the Compliance and AML Function

The reporting flows of the Compliance and AML Function to the Surveillance Body consist of annual reports, describing the results of the activity carried out concerning the Model's adequacy and functioning, as well as the changes made to the processes and procedures submitted to the Function's examination (to this end, making use of the cooperation of the Planning, Outsourcing Control and Operational Coordination Function) as well as the planned corrective and improvement actions (including training actions) and their progress. This information flow also contains indications on the activities carried out by the structure in its capacity as Anti-Money Laundering function, on the initiatives undertaken, on the dysfunctions ascertained and the relevant corrective actions to be taken, as well as on staff training activities; as required by the Group Anti-Corruption Guidelines, the Surveillance Body is also sent a copy of the Compliance Report drawn up in accordance with the legislation in force, within which the information on the control of corruption risk is also provided.

4.4.3 Information flows from the Internal Auditing Function

The ordinary reporting flow from the Internal Auditing Function to the Surveillance Body shall consist of six-monthly and annual reports, informing the Surveillance Body of the checks carried out, and the control actions planned for the subsequent six months, in line with the Annual Audit Plan. Within the scope of the reporting flow, summary evidence is provided for notifications that, upon further investigation, displayed matters relevant to Legislative Decree No. 231/2001.

Evidence is also provided of the outcome of audits carried out on the outsourcing of important or essential operational functions outside the Group (so-called FOI or FEI).

Where it deems it necessary, the Surveillance Body shall request from the Internal Auditing Function a copy of the detailed report in order to review specific matters it wishes to address more in depth.

4.4.4 Information flows from the Risk Management function

The periodic reporting flows from the Risk Management function to the Surveillance Body consist of the annual report of the risk management function, drawn up in accordance with the implementing regulation of the AIFM Directive (Directive 2011/61/EU), which summarises the checks carried out, the results found, the weaknesses detected and the actions to be taken for their removal.

4.4.5 Information flows from the Employer pursuant to Legislative Decree No. 81/08

The reporting flow from the Employer pursuant to Legislative Decree No. 81/2008 to the Surveillance Body consists of reports with at least annual frequency describing the results of the activity carried out having regard to organisation and to the controls performed on the company's Health and Safety management system.

4.4.6 Information flows from the Principal pursuant to Legislative Decree No. 81/2008

As a rule, at Neva SGR the situation of Principal pursuant to Article 88 *et seq.* of Legislative Decree No. 81/2008 does not arise. Should such an eventuality arise, a reporting flow will be produced to the Surveillance Body concerning the organisation and controls carried out on the company's health and safety management system at temporary or mobile construction sites.

4.4.7 Information flows from the Environmental Affairs Officer

The reports submitted by the Environmental Affairs Officer pursuant to Legislative Decree No. 152/06 to the Surveillance Body are focused on the annual report on compliance with the provisions of the environmental laws and the monitoring of any legislative amendments and changes, as well as the outcome of the organisation and control activities as applied to the environmental management system.

4.4.8 Information flows from the Planning, Outsourcing Control and Operational Coordination Function

The reporting flow of the Planning, Outsourcing Control and Operational Coordination Function consists of periodic reporting on:

- the main changes in the organisational structure, their significance pursuant to Legislative Decree No. 231/2001 as well as the degree of alignment of the system of delegated powers;

- a summary of the administrative expenses (quarterly) incurred by the Company, in which any deviations from what was budgeted for the period are also highlighted.

The above-mentioned report is provided to the Surveillance Body in its capacity as Board of Auditors when it is presented to the Board of Directors.

4.4.9 Further information flows

For activities relating to the management of human resources, the Intesa Sanpaolo outsourcer prepares at least once a year a report on any disciplinary measures taken against staff during the reference period (to be sent by the end of the first half of the following year), with particular evidence of events directly or indirectly linked to reports of unlawful conduct provided for in the Decree or violations of the Model.

5 THE SANCTIONS SYSTEM

5.1 General principles

Model effectiveness is ensured – in addition to the adoption of decision-making and control mechanisms such as to eliminate or significantly reduce the risk of commission of the crimes and administrative offences covered by Legislative Decree No. 231/2001 – by the disciplinary instruments established to control compliance with the required conduct.

The conduct of Neva SGR personnel (including those employed and/or operating abroad) and of external parties (meaning self-employed or para-subordinate workers, freelance professionals, consultants, agents, suppliers, and business partners) that does not comply with the principles and rules of conduct prescribed in this Model – including the Code of Ethics, the Group's Internal Code of Conduct, the Anti-Corruption Guidelines of the Group, and the internal procedures and rules that are an integral part of the Model – constitutes a contractual offence.

Based on this premise, the Company shall adopt:

- towards its employees in service through a contract governed by Italian law and through national bargaining agreements for the sector, the system of sanctions laid down in the Disciplinary Code and in the applicable laws and regulations on contracts;
- towards its employees recruited abroad and in service through a local contract, the system of sanctions established by the laws, regulations and provisions on contracts governing the specific type of employment relationship;
- towards external parties, the system of sanctions laid down in the contractual and legal provisions governing this area.

The initiation – on the basis of reports received from the corporate control functions, the Internal Auditing Function and/or the Surveillance Body –, the conduct and definition of disciplinary proceedings against employees are entrusted, within the powers assigned, to the outsourcer Intesa Sanpaolo, which supports the Chief Executive Officer in defining and issuing sanctions. The penalties against external parties shall be implemented by the function that manages the contract or with which the self-employed worker or the supplier works.

The type and size of each of the sanctions established shall be defined, pursuant to the above-mentioned legislation, taking into account the degree of recklessness, lack of judgement, negligence, fault, or wilfulness of the conduct relating to the action/omission, also considering any repetition of the misconduct, and the work activity carried out by the person concerned and his functional position, together with any other relevant circumstances characterising the fact.

Such disciplinary action shall be pursued regardless of the initiation and/or performance and finalisation of any criminal judicial action, since the principles and the rules of conduct laid down in the Model are adopted by the Company in full autonomy and independently of any criminal offences which said conduct may determine and which it is for the judicial authority to ascertain.

The Surveillance Body is responsible for verifying the adequacy of the system of sanctions and constantly monitoring the application of sanctions to employees, and the actions in respect of external parties. The Surveillance Body shall also receive from the structures concerned (Intesa Sanpaolo outsourcer for human resources management activities, Internal Auditing or the Chief Executive Officer) a report on any disciplinary measures taken against employees during the reporting period.

The system of sanctions envisaged for employees (professional areas, middle managers and executives) serving under an employment contract governed by Italian law is detailed below.

5.2 Professional and middle management staff

The sanctions system provided for professional areas and middle management includes the following:

- the measure of a verbal warning which applies in the event of minor breach of the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the sensitive areas, of a conduct which is not in line with or not appropriate to the requirements of the Model, such conduct is equivalent to a "*slight breach of the contractual rules, company rules or of the*

directives or instructions issued by management or by one's superiors" in the formulation already provided in point a) of the current Disciplinary Code;

- the measure of a written warning, which applies in the event of failure to comply with the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the sensitive areas, of a conduct which is not in line with or not appropriate to the requirements of the Model, where such non-compliance is assessed to be neither minor nor serious, such conduct is equivalent to a "non-serious breach of the contractual rules, company rules or of the directives or instructions issued by management or by one's superiors" in the formulation already provided in point b) of the current Disciplinary Code;
- the measure of suspension from service and from salary up to a maximum of 10 days, which shall apply in the event of failure to comply with the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the sensitive areas, of a conduct which is not in line with or not appropriate to the requirements of the Model, where such non-compliance is assessed to be relatively serious and/or has occurred repeatedly, such conduct is equivalent to a "*repeated or relatively serious breach of the contractual rules or of the directives and instructions issued by management or by one's superiors*" in the formulation already provided in point c) of the current Disciplinary Code;
- the measure of dismissal for justified reason, which applies in the event of the adoption, in performance of the activities belonging to the sensitive areas, of a conduct characterised by serious non-compliance with the requirements and/or the procedures and/or the internal rules laid down in this Model, where it is even simply liable to give rise to one of the offences covered by the Decree, correlating said behaviour to a " *violation (. . .) such as to constitute (. . .) a "significant" non-fulfilment of the relative obligations*" pursuant to the provisions of point d) of the current Disciplinary Code;
- the measure of dismissal for just cause shall apply in the event of the adoption, in performance of the activities belonging to the sensitive areas, of a conduct wilfully in contrast with the requirements and/or the procedures and/or the internal rules laid down in this Model, which, albeit it is simply liable to give rise to one of the offences covered by the Decree, impairs the relationship of mutual trust which characterises employment relationships, or is so serious as to impede continuation of employment, even temporarily, as such conduct is linked to an "*infringement/fault of such seriousness (either because the act was intentional, or on account of its criminal or monetary consequences, or for its repeated occurrence or its particular nature) that it impairs the trust on which an*

employment relationship is based and prevents the continuation of employment" in accordance with point e) of the current Disciplinary Code.

5.3 Executives

Where executives infringe the internal principles, rules and procedures set out in this Model or adopt, in performing the activities belonging to the sensitive areas a conduct not in line with the requirements of the Model, such persons shall incur the measures indicated below, which shall be applied having due regard to the seriousness of the infringement and to whether it is a repeat occurrence. Also in consideration of the particular fiduciary relationship existing between the Company and executive level employees, in compliance with the applicable provisions of the law and with the National Collective Employment Contract for Executives in credit companies, dismissal with notice and dismissal for just cause shall be applicable for the most serious infringements.

As said measures involve termination of the employment relationship, the Company, acting in accordance with the legal principle of applying a graduated scale of sanctions, reserves the right, for less serious infringements, to apply the written warning – in cases of mere failure to apply the principles and rules of conduct set out in this Model or of infringement of the internal rules and procedures set out and/or referred to, or of adoption, within the sensitive areas, of a conduct non complying with or not appropriate to the requirements of the Model – or alternatively, to apply suspension from work without pay for up to 10 days – in the event of negligent infringement of duty to a non-negligible degree (and/or repeated) or of negligent conduct infringing the principles and rules of conduct provided for by this Model.

5.4 Employees in service under a foreign contract

For employees in service under a foreign contract the system of sanctions is that envisaged in the local regulations specifically applicable.

5.5 External parties

Any conduct adopted by external parties not belonging to the Company which, in conflict with this Model, may give rise to the risk of occurrence of one of the offences covered by the Decree, shall, in accordance with the specific terms and conditions of contract included in the letter of appointment or in the agreement, produce early termination of the contractual relationship, without prejudice to any further remedy available to the Company in the event that it suffers real damage as a consequence of such conduct, e.g. where the Judicial Authority applies the sanctions set out in the Decree.

5.6 Members of the Board of Directors

In the event of violation of the Model by persons holding the position of members of the Company's Board of Directors, the Surveillance Body shall take the initiatives deemed appropriate in proportion to the seriousness of the infringements, in compliance with the laws in force.

6 INTERNAL COMMUNICATION AND TRAINING

The administrative liability regime laid out by the law and the Organisational, Management and Control Model adopted by the Company form an overall system which must be reflected in the operational conduct of the Company's Staff.

To obtain appropriate Staff response it is essential to implement a communication and training activity for the purpose of disseminating the contents of the Decree and of the Model adopted, including all its various components (the corporate instruments underlying the Model, the aims of the Model, its structure and key components, the powers and delegation system, identification of the Surveillance Body, information flows to the Surveillance Body, the protections provided to those that report unlawful acts, etc.). The purpose is to ensure that knowledge of the subject matter and compliance with the rules arising from it become an integral part of each staff member's professional culture.

Based on this knowledge, the training and internal communications activities addressed to all the Staff have the constant objective – also in accordance with the specific roles assigned – of creating widespread knowledge and a corporate culture embracing the issues in questions, having regard to the specific activities carried out, so as to mitigate the risk of offences taking place.

6.1 Internal communication

On being hired, new staff members receive, together with the required recruitment documents, a copy of the Group's Model, Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. By signing a declaration, staff members confirm they have received the documents and have read them fully, and undertake to comply with the rules they contain.

The Company's Organisational, Management and Control Model is published and made available for consultation on the corporate intranet; in addition, the Group's intranet also contains the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines, which are adopted by Neva.

The documents published on this site are regularly updated to incorporate any intervening changes in the legislation and in the Model, the periodic updates to which are communicated to all employees.

Internal communications in support of the Decree and the Model use a variety of tools.

The Internal News Intranet site and Intesa Sanpaolo Web Tv, the latter in live and on-demand modes, are the tools used to inform staff in real time of any new developments; Web Tv, in particular, is a tool capable of offering useful opportunities for in-depth analysis of the relevant regulations, "sensitive" activities, training interventions, etc., through special broadcasts (video clips), including interviews with the various managers. The Group's in-house magazine and the publication of popular communication material (e.g. vademecum/monographic handbooks) are the tools intended to host regular in-depth articles, also written with the contribution of experts, as well as contributions concerning the Decree, the aim of which is to promote the dissemination and consolidation of knowledge on the administrative liability of entities.

In summary, all the instruments mentioned above, together with the in-house communications and circular notices, ensure that all staff members receive exhaustive and prompt information at all times.

6.2 Training

The training activities aim to make the Decree and the Model known and, in particular, appropriately support those who are involved in “sensitive” activities.

To ensure it would be effective, the training provided takes into account the many variables present in the reference context; in particular:

- the target (the addressees of the actions and their position and role in the organisation);
- the contents (subjects covered, relevant to the individuals’ roles);
- the training delivery tools (live, digital training);
- the training planning and delivery time (the time needed to prepare and implement the training actions);
- the level of commitment required of the trainees (training time);
- the actions necessary to adequately support the training action (promotion, support by the Department heads).

The training activities include:

- an e-learning training module addressed to the whole staff;
- specific training modules designed for Staff members operating in the sectors at greater risk of unlawful conduct (in particular, those working in close contact with the public administration, those operating in the Procurement or Finance Departments etc.);

- other in-depth training tools used via the training platform.

The platform, accessible to all employees,allows each participant to view the baseline training content on Legislative Decree 231/2001, as well as any updates to the legislation, and verify how much they have learned through a final examination.

The specific training modules are implemented, where necessary, after using the digital training targeted to the entire staff and whose purpose is to disseminate knowledge of the offences, possible types of offences, and specific safeguards relating to different departments, and to refer to the proper application of the Organisational, Management and Control Model. The teaching method is strongly interactive and makes use of case studies.

The digital training and targeted training contents are updated having regard to the developments in external legislation and in the Model. Whenever substantial changes take place (e.g. extension of the scope of the entity's administrative liability to include new types of offences), training contents are suitably supplemented and delivered. All staff targeted by the various training actions must participate in the training.

The use of the various training initiatives is compulsory for all the personnel to whom the initiatives are addressed and is monitored by the competent Human Resources function of the outsourcer, with the cooperation of the Managers at the various levels of the structures to which they belong, who must ensure, in particular, that their collaborators use the "distance learning" training initiatives.

The Planning, Outsourcing Control and Operational Coordination Function is responsible for collecting data on staff participation in the various programmes and archiving it, making it available to the functions concerned.

The Surveillance Body shall monitor the progress of the training activities also by means of the information forwarded by the Compliance and AML Function, and may request periodic checks on the staff's level of knowledge of the Decree, of the Model and of its operational implications.

7 PREDICATE OFFENCES - AREAS, ACTIVITIES AND ASSOCIATED RULES OF CONDUCT AND CONTROL

7.1 Identification of the sensitive areas

Article 6, paragraph 2 of Legislative Decree No. 231/2001 provides that the Model shall "identify the activities within which offences may be committed".

The predicate offences covered by the Decree have also been analysed, as illustrated in paragraph 2.4; the business areas of the Company which are at risk of offences being committed have been identified for each category.

For each area, the various sensitive activities have been identified and the control principles and rules of conduct to be applied by all the persons assigned to those areas have been defined.

The Model is fully implemented in the Company's operations by connecting each area and "sensitive" activity with the corporate structures concerned and with the dynamic management of the processes and of the relevant reference rules.

Under the provisions of the law currently in force, the sensitive areas identified by the Model concern, in general:

- Sensitive area concerning offences against the Public Administration;
- Sensitive area concerning corporate offences;
- Sensitive area concerning receipt of stolen goods, money laundering and use of unlawfully obtained money, goods or benefits, as well as self-laundering;
- Sensitive area concerning crimes with the purpose of terrorism and subversion of the democratic order, organised crime, transnational crimes and crimes against the person, as well as sports fraud and illegal betting or gaming;
- Sensitive area concerning crimes and administrative offences relating to market abuse;
- Sensitive area concerning workplace health and safety offences;
- Sensitive area concerning computer crime;
- Sensitive area concerning crimes against industry and trade and crimes involving breach of copyright and customs' law;
- Sensitive area concerning environmental crimes;
- Sensitive area concerning tax crimes.

7.2 Sensitive area concerning offences against the Public Administration

7.2.1 Type of offence

Articles 24 and 25 of the Decree concern a series of offences against the Public Administration laid down in the Criminal Code which have in common the identity of the legal asset they protect, which is the impartiality and sound management of the Public Administration.

The legislator's constant focus on fighting corruption has led to repeated interventions in this area. Over time the punishments have become harsher, new offences have been introduced while others have been amended, including the offence of "*Illegal inducement to give or promise benefits*", which was previously covered by the crime of *"Bribery*" and the offence of "*Trafficking of illegal influences*". Provision has also been made for the offences of "*Private-to-private corruption*" and "*Incitement to bribery among private individuals*", as described in Chapter 7.4. Although these are corporate offences, they belong to the wider measures to combat instances of corruption which can compromise fair competition and the proper functioning of the economic system in general. Further offences were also added for the protection of public finances, both in Italy and in the European Union (hereinafter also EU), including crimes of "Embezzlement" and "Abuse of office".

For the purposes of criminal law a Public Administration Body is defined as being any legal person that pursues and/or implements and manages public interests and which is engaged in legislative, jurisdictional or administrative activity, governed by provisions of public law and which is implemented through instruments issued by the authorities.

Purely by way of example, and with reference to the entities typically having relations with the Company, the following can be identified as being Public Administration Bodies: i) the State, the Regions, the Provinces, the Municipalities; ii) Ministries, Departments, Committees; iii) non-economic Public Bodies (INPS, ENASARCO, INAIL, ISTAT).

Among the criminal offences considered herein, the offences of extortion and undue inducement to give or promise benefits, as well as the offences of "*Bribery against the Public Administration"*, in their various types, and the offences of embezzlement and abuse of office presuppose the necessary involvement of a private individual and a public agent, i.e. a natural person who takes on, for the purposes of criminal law, the title of "Public Official" and/or "Person in Charge of a Public Service", in the meaning respectively attributed by Articles 357 and 358 of the Italian Criminal Code.

In short, it should be noted that the distinction between the two profiles is in many cases debatable and blurred, and that it is defined by the above-mentioned provisions according to criteria referring to the objective function performed by such persons.

The title of Public Official is given to those who perform a legislative, judicial or administrative public function. The exercise of an administrative public function is usually associated with those who have decision-making responsibilities or concur to the decision making process of a public body or who represent the public body in dealings with third parties, and with those exercising authoritative powers or certification powers[10].

Purely by way of example, we may mention the following persons, who have been identified by case law as being Public Officials: court bailiffs, court-appointed technical experts, receivers in bankruptcy cases, tax collectors or executives attached to municipal companies, even if in the form of an S.p.A., university assistants, postmen, officials at the Italian Automobile Club branch offices, municipal councillors, municipal surveyors, public school teachers, health service officials, notaries and employees of the Italian Social Security Agency, authorised Local Health Service doctors, tobacconists authorised to collect vehicle tax.

The title of Public Service Officer is assigned by exclusion, as it goes to those who perform public interest activities, not consisting of simple or merely material tasks, governed in the same manner as public function, but which do not entail the powers typically assigned to a Public Official.

Purely by way of example, we may mention the following persons, who have been identified by case law as being a Public Service Officer: payment collectors of the National Electricity Company (Enel), gas and electricity meter readers, post office clerks tasked with sorting correspondence, employees of the Italian State Mint, security guards responsible for cash consignments.

It should be noted that under the law, for the purpose of being classified as a Public Official or a Public Service Officer, a person does not necessarily have to be an employee of a Public Body: this because in certain particular cases, a public function or public service may also be performed by a private person[11].

Therefore, employees and officers of the Company who in exercising the above-mentioned duties of public importance adopt conduct typical of public agents as described for the offences of "*Bribery against the Public Administration*", extortion and illegal inducement to

[10] The concept of "authoritative powers" includes not only coercive powers, but also any discretionary activity carried out in respect of persons who are not on the *same level* as the authority (see Court of Cassation, Joint Sections, ruling 181 of 11/07/1992). The certification powers cover all the activities relating to the issue of documentation having the power of proof under the law, whatever their level.

[11] In particular, activities relating to the placement of public debt securities, tax collection, treasury services for a Public Body, investment financing, special or soft loans, can, according to case law, take on public service relevance to the point that the Bank's employees and managers may, in performing those activities, take on the title of public agent, at least as a Public Service Officer.

give or promise benefits are punished as such and can also trigger the Company's liability under Legislative Decree No. 231/01.
The liability of the officers and employees, as well as the entity, can also arise if they adopt conduct with public agents typical of private individuals as described for the above-mentioned offences.

Under Article 322-bis of the Criminal Code, the conduct of the private individual – whether as bribe-giver, instigator or as the party induced to give or promise benefits − is a punishable criminal offence not only when involving Public Officials and Persons in Charge of a Public Service within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international public organisations, supranational organisations, international parliamentary assemblies or international courts.

The criminal offences laid down in Articles 24 and 25 of the Decree are summarised below[12].

Embezzlement (Article 314, paragraph 1, and Article 316 of the Criminal Code)
The offence is committed by a public official or a public service officer who appropriates money or movable property of others that has come into his possession or has become available for the purposes of service, or who receives or unduly retains money or other benefits for himself or other parties, perceived by taking advantage of the error of others.
Such conduct involves administrative liability pursuant to Legislative Decree No. 231/2001 only if the facts harm the financial interests of the EU.
These are disputable offences in situations where the elements of other offences do not occur, such as fraud against the EU.
In banking operations, the offence could be committed by the employee who appropriates, directly or in conjunction with other subjects, also for the benefit of the Company, sums collected from or intended for customers, when carrying out activities of a public nature, for example in the sector of public financing with EU funds.

Abuse of office (Article 323 of the Criminal Code)

[12] Articles 24 and 25 of Legislative Decree No. 231/2001 were modified by Article 5 of Legislative Decree No. 75/2020 which, starting from 30 July 2020, introduced the new predicate offences of embezzlement, abuse of office, fraud in public supplies, undue receipt of FEA disbursements, fraud and IT fraud against the EU.

The law punishes any conduct relating to the functions of a public official or public service officer that does not fall within more serious criminal offences, but which in any case is characterized by the intention to procure an unfair financial advantage for oneself or others or to cause others unfair harm. The conduct must be characterized by:

- the violation of specific rules of conduct expressly provided for by law or by acts having the force of law, from which there is no margin of discretion in decisions;
- the presence of conflict with one's own interest or that of a close relative or other situations which by law require abstention from carrying out the activity.

Such conduct involves administrative liability pursuant to Legislative Decree No. 231/2001 only if the facts harm the financial interests of the EU.

In banking operations, these cases could occur when carrying out activities of a public nature, for example in the sector of public financing with EU funds or in a competition with a public official who carries out an undue ruling in favour of the Company, at the request of Company staff aware that they are not entitled, even in the absence of promises or donations, which would otherwise constitute crimes of corruption.

Misappropriation of Public Funds (Article 316-bis of the Criminal Code)

This offence occurs when, after having lawfully received financing, subsidies or contributions, subsidised loans or other disbursements of the same type, however denominated, from the Italian Government or other public body of the European Communities for the execution of works or activities in the public interest, the sums are not used for the purposes for which they were granted. In the context of the Company's operations, the offence in question may occur both in the event that the subsidies are disbursed in favour of the Company for its direct benefit, and in the event that the Company intervenes in the process of disbursing the subsidies in favour of the private recipients who are the authors of the diversion from the predetermined public purposes and in complicity with the customer.

Unlawful receipt of Public Funds (Article 316-ter of the Criminal Code)

The offence occurs in cases where – through the use or presentation of false statements or documents or through the omission of required information – contributions, financing, subsidised loans or other disbursements of the same type, granted or disbursed by the State, other public bodies or the EU, are obtained without being entitled thereto. The use to which the disbursements are put is irrelevant, since the offence is committed at the time the funding is obtained. The conduct is punished more severely if it affects the financial interests of the EU and the damage or profit exceeds €100,000.

This offence, too, can occur either where the beneficiary of the grants is the Company itself or where the Company acts as intermediary in favour of customers responsible for the false declarations or omissions and aids and abets them.

Disturbing the freedom of invitations to tender (Article 353 of the Criminal Code)

Disturbing the freedom to choose a contractor (Article 353 bis of the Criminal Code)[13]

The first offence punishes anyone who, by means of violence or threats, or by gifts, promises, collusion or other fraudulent means, prevents or disrupts tenders in public auctions or private tenders on behalf of public administrations, or drives away the bidders. The offence, albeit with an attenuated penalty, is also committed in the case of private tenders on behalf of private persons directed by a public official or legally authorised person. Since it is a danger offence, it takes shape not only in the case of actual damage, but also in the case of mediated and potential damage, since the actual achievement of the result pursued by the perpetrators of the offence is not required, but merely the fact that such acts can influence the progress of the tender.

The second offence punishes anyone who, unless the offence constitutes a more serious offence, with violence or threats, or with gifts, promises, collusion or other fraudulent means, disturbs the administrative procedure aimed at establishing the content of the call for tenders or other equivalent act, in order to influence the manner in which the Public Administration chooses the contractor. This offence concerns the phase of calling for tenders and, more precisely, that of approving the call for tenders, and punishes the conduct of those who, with the collusion of the contracting authority, seek to have calls for tenders drawn up in such a way that they contain such stringent requirements as to predetermine the number of potential competitors (so-called “tailored tender specifications").

Undue receipt of payments from the European Agricultural Fund (Article 2 of Law No. 898/1986)

This provision punishes anyone who obtains for himself or for others aid, bonuses, allowances, refunds or payments in general, even if only partially, from the European Agricultural Guarantee Fund or the European Agricultural Fund by showing false data or information. These disbursements are equivalent to the national quotas in addition to those disbursed by the aforementioned Funds, as well as the disbursements made entirely by national finance on the basis of relevant EU legislation.

[13] These predicate offences were introduced by Article 6 *ter* para. 2 of Legislative Decree No. 105 of 10 August 2023, converted into Law No. 137/2023, published in the Official Gazette on 9 October 2023, by amending Article 24, paragraph 1 of Legislative Decree No. 231/2001.

When the conduct does not only refer to false information, but also to tricks or deceitful deceptions, it considered as a more serious crime of fraud against the State.

Fraud in public supplies (Article 356 of the Criminal Code)

The offence is committed by anyone who fails to fulfil their obligations in the execution of supply contracts with the State, with another public body or with a company providing public services or services for public requirements, by resorting to artifices or deceptions such as to deceive the counterparty over the content of its service, by making all or part of the objects or works necessary for a public establishment or a public service missing.

The penalty is increased if the supply concerns foodstuffs or medicines, or objects or works intended for communications, arms or equipment of the armed forces, or to remedy a common danger or public incident.

Fraud against the State or another public body (Article 640, paragraph 2, 1 of the Criminal Code)

This type of offence occurs when an unfair profit is obtained by means of artifices or deceits aimed at misleading and causing damage to the State, another Public Body or the European Union.

This offence occurs, for instance, when, in preparing the documents or data required for participating in a tender procedure, the tenderer provides the Public Administration with false information supported by forged documents in order to be awarded the contract.

Aggravated fraud for the purpose of obtaining public funds (Article 640-bis of the Criminal Code)

This type of offence occurs when the fraud is carried out for the purpose of unduly obtaining public funds from the State, other Public Bodies or the European Union.

The distinguishing features of this offence are the following: compared with the generic fraud offence (Article 640, paragraph 2, 1, of the Criminal Code), this offence is characterised by its specific material object, which is obtaining public funds, howsoever named; compared with the unlawful receipt of public grants (Article 316-ter of the Criminal Code), this offence is characterised by the additional use of some artifices or deceits to mislead the granting authority.

Computer fraud (Article 640-ter of the Criminal Code)

Computer fraud consists of altering the functioning of an IT or telecommunications system or of tampering with the data or software contained therein, obtaining unfair profit. It is relevant for the purposes of Legislative Decree No. 231/2001, only where it is perpetrated to the detriment of the Government, other Public Body or the EU.

Given the characteristics of the Company's business, this offence tends not to occur.

Extortion in office (Article 317 of the Criminal Code)

An active role in the offence of extortion can be played by a Public Official or a Public Service Officer who, abusing of his/her office or powers, forces someone to give or promise to him/her or a third party money or other undue benefits.

The coercion takes the form of violence or threats of undue harm (for example: a refusal to perform an action unless paid to do so), by means that do not leave the freedom of choice to the coerced individual, who is consequently considered the victim of the offence and exempt from punishment.

As explained in the introduction, in relation to the activities carried out, Neva's corporate officers and employees cannot be qualified as “Public Officials" or as Persons in Charge of a Public Service, therefore, the offence in question could be committed in the event that the senior or subordinate person engages in extortionary conduct in complicity with a Public Official or a Person in Charge of a Public Service against a third party[14].

Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)

This offence punishes the conduct of a Public Service Officer or a Public Official who, abusing of his/her office or powers, induces another person to give or promise to him/her or to a third party money or other undue benefits.

This is an offence different than that of extortion: the pressure and demands of the public agent are not in the form of moral violence typical of extortion, but instead assume forms of mere conditioning of the will of the counterparty, such as describing the potential unfavourable consequences or difficulties, stonewalling, etc. the conduct of the person submitting to the inducement, paying or promising undue benefits to avoid damage or to achieve unlawful advantage, is also punished. This conduct is punished more severely if it affects the financial interests of the EU and the damage or profit exceeds €100,000.

As explained in the introduction, in relation to the activities carried out, Neva's corporate officers and employees cannot be qualified as "Public Official" or "Person in Charge of a Public Service", therefore, the liability of the Company for illegal inducement can be configured, provided that the interest or advantage of the entity exists, in the case of an

[14] The liability of the entity may therefore arise, provided that the interest and advantage of the latter exist, if at the time of the commission of the offence the senior or subordinate person was aware, or should reasonably have been aware, of the qualification assumed by the Public Official or the Person in Charge of a Public Service.

offence committed by a senior or subordinate person according to one of the following alternative forms:

- inductive conduct adopted in concert with a Public Official or with a Public Service Officer against a third party[15];
- acceptance of inductive conduct from a Public Official or Public Service Officer.

Bribery

The element common to all cases of bribery against the interests of the public administration consists in an agreement between a public agent (Public Official or a Public Service Officer) and a private individual.

The corrupt agreement presupposes that the counterparties act on an equal footing, regardless of which of the two parties initiated the bribery, unlike the situation in cases of extortion in office and illegal inducement to give or promise benefits, which instead requires that the person holding the public office, abusing of such office, exploits his/her superior position vis-à-vis the private party who is in a state of inferiority. Moreover, it can prove difficult in practice to distinguish between instances of bribery and illegal inducement; the distinction is important first and foremost to determine the punishment to be inflicted upon the private individual, which is milder for illegal inducement.

In bribery, two separate offences are distinguished: one is committed by the person receiving the bribe, who holds the public office (passive bribery), the other is committed by the bribe-giver (active bribery), which under the provisions of Article 321 of the Criminal Code shall be punished with the same penalties envisaged for the person receiving the bribe. The Company may be liable for this type of offence committed by its managers or employees, also in its interest or for its benefit in the case of both active and passive bribery.

As explained in the preamble, in fact, it is not considered possible to attribute the status of public servant to the employees of the Company in view of the fact that the activities carried out do not qualify as “activities of public relevance".

The following types of bribery are covered by Article 25 of the Decree.

Bribery relating to the exercise of duties (Article 318 of the Criminal Code)

This type of offence occurs when a Public Official or a Public Service Officer receives, for his/her own benefit or for the benefit of others, money or other benefits, or accepts a promise thereof, for performing his/her own duties or exercising his/her own powers. The activity of the public agent can concern either a required act (for example: fast-tracking a

[15] The liability of the entity may therefore arise if, at the time of the commission of the act, the senior or subordinate person was aware, or should reasonably have been aware, of the qualification assumed by the Public Official.

procedure which comes under his responsibility), but the offence also exists if the illegal benefit is:

- paid or promised regardless of the identification of a "purchase or sale" in a well-defined act, in that the mere fact that it arises in relation to the general exercise of duties is sufficient;
- paid after an official duty is performed, even if it was not previously promised.

Consequently, there are extensive and widely diverse scenarios of subservience to the duty and of donations giving a generic appearance of preferential treatment[16].

Bribery relating to an act contrary to official duties (Article 319 of the Criminal Code)

This offence, also known as "direct corruption", consists of an agreement relating to the promise or giving of undue payment in relation to an act, to be performed or already performed, that is contrary to the official duties of a public agent (for example, a cash payment for ensuring the award of a contract in a competitive tendering procedure).

Bribery in judicial proceedings (Article 319-ter, paragraph 1 of the Criminal Code)

In this type of offence, the conduct of the bribed person and of the bribe-giver is characterised by the specific aim of favouring or damaging one of the parties to criminal, civil or administrative proceedings.

Incitement to bribery (Article 322 of the Criminal Code)

This offence is committed by a private party whose offer or promise or money or of other benefits for the exercise of public office (Article 318 of the Criminal Code) or of an act contrary to official duties (Article 319 of the Criminal Code) is rejected. The same offence applies to a Public Official or a Public Service Officer who solicits such offer or promise without obtaining it.

Trafficking of illegal influences (Article 346-*bis* of the Criminal Code)[17]

A person is guilty of this offence if, by exploiting or asserting existing or alleged relations with a public official or public service officer – or with anyone performing corresponding functions within the European Union, third countries, international organisations or courts –

[16] Article 318 of the Criminal Code prior to the "anti-corruption law" only contemplated the instance of "improper bribery", i.e. undue payment for performing a specific act, due or in any event compliant with official duties of the public agent. Paragraph 2 envisaged the conduct of "improper bribery after the fact", i.e. undue payment not previously agreed but paid after performance of a specific official act, in which case the person receiving the bribe was punished but not the bribe-giver. Following the repeal of that paragraph, the aforementioned conduct qualifies as under paragraph 1, and consequently both are now punished under such circumstances (see Article 321 of the Criminal Code). Lastly, the title of public employee of the Public Service Officer, which was required in order for the offence in question to apply, is no longer relevant.

[17] This offence was introduced into the Criminal Code by law 190/2012 and was then amended by law 3/2019, which added it to the predicate offences covered by Article 25 of Legislative Decree No. 231/2001 with effect from 31.1.2019.

makes an undue promise or gift of cash or other benefits for themselves or for others, as the reward for their illegal mediation, or to remunerate them for the exercise of their duties. Anyone who makes an agreement with the intermediary in relation to this illegal influence will be punished in the same way.

The punishment is harsher in those cases in which the "vendor" of influential relations, whether real or only claimed, is a public official or person in public service, or in cases in which there is an influence on the exercise of judicial activities, or where the objective is to remunerate a public official or a public service officer to perform an act that conflicts with their official duties, or to omit or delay an official act.

The illegal influence does not have to be actually exercised, for the offence to exist; where this does occur, and where the requirements for the corruption offences governed by Articles 318, 319 and 319-*ter* are met, the parties to the illegal agreement will be punished not by Article 346-*bis*, but on the grounds of conspiracy to commit such offences. This is an offence intended to prevent and punish even the risk of any corruptive agreements taking place.

The law also punishes intermediation through the exercise of public functions – in other words to carry out acts that do not conflict with public duties – which may be a prelude to the corruptive agreements punishable under Article 318 of the Criminal Code. However, lobbying to represent personal interests or to present defence arguments to the authorities through trade associations or qualified professionals, is considered legitimate provided that it is done transparently and correctly, and not in order to obtain undue favours.

7.2.2 Sensitive company activities

The sensitive activities identified in the Model which involve the highest risks of unlawful conduct in relations with the Public Administration are the following:

- Signing contracts with the Public Administration;
- Managing contractual relations with the Public Administration;
- Management of activities relating to a request for authorisation or fulfilment of requirements towards the Public Administration;
- Management and use of the Group's IT systems and Information assets;
- Management of public subsidy schemes;
- Management of funded training;
- Management of litigation and out-of-court settlements;
- Management of relations with the Supervisory Authorities;
- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants;

- Management of gifts, entertainment expenses, donations to charities and sponsorships;
- Management of the staff selection and recruitment process;
- Management of relations with regulatory bodies.

We reproduce below, for each of the above-mentioned sensitive activities, the protocols laying down the control principles and rules of conduct applicable to these activities, as well as the detailed corporate regulations governing such activities.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.2.2.1 Entering into contractual relations with the Public Administration

This protocol applies to all the Company Structures involved in the signing of any type of contracts with Public Administration Bodies, concerning transactions such as, but not limited to:

- entering into contractual relationships with Public Bodies arising from the subscription of units of Funds managed by the Company;
- entering into contractual relationships with Public Bodies resulting from participation in tenders or applications for public funding, grants or other disbursements;
- conclusion of corporate contractual relationships and shareholders' agreements with Public Bodies, for the purpose of establishing and managing equity investments;
- support from consultants prior to the signing of contractual relationships with the Public Administration;
- financial, strategic and business advisory and consultancy services.

Pursuant to Legislative Decree No. 231/2001, the contract signing process could present opportunities for the offences of "bribery against the Public Administration", in its various forms, of "Illegal inducement to give or promise benefits", "Trafficking of illegal influences"[18], "Fraud against the State or other public body", "Fraud in public supplies", "Disturbing the freedom of invitations to tender" and "Disturbing the freedom to choose a contractor".

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The process for the signing of contracts with the Public Administration comprises the following steps:

- commercial development activity and identification of business opportunities;
- managing pre-contractual relations with the Public Administration;
- participation (where required) in public or private tendering procedures for the award of the services including:
    - preparing and approving the documentation and forms necessary for participating in the tender procedures;

[18] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves public officials and public service providers within the Italian public administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts

- submitting the application for participation in the tender procedure to the Public Body of reference;
- preparing and approving the documentation and forms necessary for submission of the commercial offer to the Entities;
- submission of the technical and economic offers to the Public Body of reference;

- conclusion of the contract with the Entity (preparing all the information necessary for the subsequent management of the contract).

The operating procedures for management of the process are governed by the Company and Group internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - persons exercising authorisation and/or negotiating powers with the Public Administration:
    - are specifically identified and authorised on the basis of the specific role attributed to them in the Company's Organisational Manual and Functional Chart and in the internal system of powers and delegations; such persons may only appoint third parties to hold relations with public bodies on the basis of specific ad hoc delegations to be kept by the structure itself;
    - only operate within the scope assigned to them by the head of the reference structure;
  - deeds that contractually bind the Company must only be signed by persons specifically authorised by virtue of the existing system of delegations or powers or specifically identified by the Board of Directors;
  - the power and delegation system establishes management autonomy levels according to type of expenditure and size of the commitment, including towards the Public Administration; internal regulations illustrate the aforementioned authorisation mechanisms, providing an indication of the corporate officers holding the necessary powers.
- Segregation of duties between the persons involved in the process of defining the contractual agreement with the Public Bodies and the use of company funds. Specifically:
  - definition of the agreement is exclusively entrusted to the Head of the Corporate Structure which is competent by reason of the subject of the contract or to duly

empowered persons; formal conclusion of the contract shall take place in accordance with the current power and delegation system;

- the use of company funds is regulated by internal operating procedures that require, for amounts exceeding certain thresholds, the intervention of several persons in charge of carrying out the various phases of the transaction (entry/authorisation), according to the maker and checker principle. Control activities:
  - the documentation relating to conclusion of the contractual relationships is submitted for review to the Head of the Corporate Structure which is competent by reason of the subject of the contract or to duly empowered persons who, for the purpose of defining new types of contracts, shall avail themselves of the advice of the competent Group Structure with regard to legal aspects;
  - all the documentation prepared by the Company for participation in public calls for tenders must be checked, for material and formal truthfulness and congruence, by the Head of the Corporate Structure competent by reason of the subject of the contract or by duly empowered persons.
- Process traceability including both the electronic and the paper trail:
  - each key phase of the agreements with the Public Administration must be recorded in writing;
  - any agreement/convention/contract with Public Bodies shall be formalised in a document, which shall be duly signed by persons holding the required powers under the current power and delegation system or by persons specifically delegated by the Board of Directors;
  - in order to allow reconstruction of the responsibilities and of reasons for the choices made, each Structure shall be responsible for filing and storing the documentation falling under its competence, in telematic or electronic format, as well as the final agreements/covenants/contracts as part of the activities relating to the process of entering into contracts with the Public Administration.
- Bonus or incentive systems: bonus and incentive systems of the Company must be able to guarantee compliance with legal and Group provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of conduct

The Company's structures howsoever involved in the activities relating to the conclusion of contractual relationships with the Public Administration, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any

provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. Specifically:

- all persons that, during the phase of commercial development and identification of new business opportunities, enter into relations with the Public Administration on behalf of the Company, must be identified and authorised in accordance with the specific role assigned to them in the Organisational Manual and the Functional Chart or by the Head of the reference Structure by means of an internal written authorisation kept on record by the Structure in question;
- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Company must be expressly appointed;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing Function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- if third parties are to be involved in the process for the conclusion of the contractual relationships with the Public Administration, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001 and the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- produce incomplete documents and/or communicate false or altered data and/or omit relevant information on the characteristics of individual transactions;
- adopt deceitful conduct which might lead Public Bodies into error in their choice of procuring services from the Company or in respect to the characteristics of bank and financial products/services;
- ask or induce - including through intermediaries - members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the decision to conclude agreements/covenants/contracts with the Company or disturb

the administrative procedure aimed at establishing the content of a call for tenders or other equivalent act in order to influence the manner in which the Public Administration chooses a contractor;

- promise or pay/offer - including through intermediaries - undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Company's interests. Examples of such improper advantages include, without limitation, the promise to hire family members and relatives, sponsorship or charity initiatives in favour of related persons, incentives granted in violation of applicable and company regulations, and more generally, all banking or financial transactions which generate a loss for the Company and a profit for the aforementioned persons (e.g. unjustified cancellation of a debt position and/or application of discounts or conditions not in line with market parameters);
- promise to pay/offer undue sums of money, gifts or services in kind, benefits of any nature, as described in the previous paragraph, in favour of senior officers or their staff of companies/entities participating in public or private tenders with a view to persuading them not to participate or to learn of their bids and formulate them in such a way as to ensure they are awarded the contract, or threatening them with unfair damage for the same reasons;
- award appointments to any external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of committing offences of *"Bribery against the Public Administration"*, in their various forms, and of "*Illegal inducement to give or promise benefits*" and the "*Trafficking of illegal influences*" which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating the establishment/development of relationships aimed at award of the contract.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.2 Management of contractual relations with the Public Administration

This protocol applies to all the Company Structures involved in the management of contractual relationships with Public Administration bodies, concerning transactions such as, but not limited to:

- management of agreements concerning the establishment and management of equity investment relationships or subscription of shares by Public Bodies;
- management of loans/contributions or other public funds obtained by the Company for any reason;
- management of financial, strategic and business advisory and consultancy relationships;
- management of the applications and subsequent receipt of contributions/facilities supporting subsidised financing.

Pursuant to Legislative Decree No. 231/2001, the relevant processes could present opportunities for the commission of the offences of "*bribery*", in their various types, of "*Illegal inducement to give or promise benefits*"[19], of "*Trafficking of illegal influences*" , of "*Extortion*" of "*Fraud against the State or other public body*", "*Misappropriation*", "*Misappropriation of public funds*", "*Embezzlement*", "*Abuse of office*", "*Unlawful receipt of payments from the European Agricultural Fund*" and "*Fraud in public supplies*".

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The process of managing service agreements for the placement of investment fund units with Public Bodies consists of the following steps:

- collection of the subscription request;
- verification of the prerequisites for the customer's admission to subscription;
- confirmation to the customer (or possible rejection) of the subscription request.

The management of agreements concerning the establishment and management of equity investment relationships or the subscription of units by Public Bodies is broken down as follows:

- preliminary analysis of the requirements for performing of the contract;
- performance of the contract;

[19] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

- monitoring of contract performance.

The process of managing loans/contributions or other public funds obtained by the Company for any reason tends to consist of the following stages:

- preliminary verification of eligibility based on regulatory requirements;
- preparing the accounting prospectuses/applications for the contributions and submitting it to the Authority;
- collection of funding/contributions from the Authority;
- management of funding and contributions received;
- clearance of accounts.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - the management of relations with the Public employees during performance of the contractual obligations assumed towards the Entities themselves is delegated to specific structures of the Company on the basis of the system of delegations and powers in place. Contracts for the provision of services to the Public Administration are concluded in accordance with the rules of conduct set out in the Protocol for the "Conclusion of the contractual relationships with the Public Administration". In particular, all acts whereby the Company accepts a contractual obligation towards third parties can only be signed by specifically authorised persons;
  - within each structure, the persons involved in the management of contractual relations with the Public Administration must be identified and authorised on the basis of their specific role by the Company's functional chart or Organisational Manual, or by the Head of the Structure concerned in the exercise of his/her powers, and must operate exclusively within the perimeter assigned to them.
- Segregation of duties between the persons involved in the process of managing contractual agreements with Public Bodies. Specifically:
  - the persons tasked with preparing the reporting documents to be submitted to the public bodies shall be different from those who sign such documents;
  - those who produce the documentation to be submitted are different from those who deal with External Authorities;

- the persons who account for the transaction are different from those who deal with the Public Administration.

- Control activity by each competent structure and in particular:
  - verification of the documentation to be submitted against the provisions of the Authority (also with reference to the documentation certifying the technical, economic and professional requirements of the Company);
  - checking the formal correctness of the documents to be submitted to the Funding Entity in order to obtain the financing or disbursement;
  - line controls performed by each Structure concerned when performing accounting/administrative activities relating to performance of the processes subject of this protocol.
- Process traceability both at the information system level and in terms of documents: each Structure from time to time concerned, in order to allow reconstruction of responsibilities, is responsible for filing and storing all the documentation produced, also in telematic or electronic format, relating to the performance of the activities carried out in the context of the process of managing relations with the Public Administration.
- Bonus or incentive systems: bonus and incentive systems of the Company and Group must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of Conduct

The Company's structures howsoever involved in the management of relationships with Public Administration Bodies arising from contractual obligations towards such Bodies shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any applicable provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process who are responsible for signing deeds or documents with relevance outside the Company, as well as the persons who, when requesting and managing public financing or contributions, have relations with the Public Administration, must have appropriate powers according to the system of powers and delegations in place or specifically delegated by the Board of Directors;
- the persons involved in the process may not follow up any request for undue advantages or attempted extortion by a Public Administration official of which they may be the recipients or which may simply come to their knowledge, and must immediately report it to their Manager, who in turn is obliged to forward the report received to the Internal

Auditing Function and to the Corporate Anti-Corruption Officer for the appropriate assessments and any possible fulfilment towards the Surveillance Body in accordance with Chapter 4.1;

- if third parties are to be involved in the process for the management/execution of contractual relationships with the Public Administration, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001 and the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- all relations with and obligations towards the Public Administration, or its representatives/officials, shall be carried out with the highest transparency, diligence and professionalism, supplying clear, accurate, complete, faithful and truthful information, and always reporting any conflicts of interest following the established procedure.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- produce incomplete documents and/or communicate false or altered data and/or omit relevant information on the characteristics of individual transactions;
- engage in misleading conduct that could mislead the financing/disbursing entities;
- use public grants, subsidies and financing for other than the purpose they have been granted for;
- ask or induce - including through intermediaries - members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the management of the relationship with the Company;
- promise or pay/offer - including through intermediaries - undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one’s own behalf or for others − to representatives of the Public Administration in a personal capacity in order to further or favour the Company’s interests. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons, the payment of incentives in violation of the reference rules and company regulations and, more generally, all those financial

transactions that result in the generation of a loss for the Company and the creation of a profit for the aforementioned persons;

- receive money, gifts or any other benefits or accept the promise of such benefits from any person attempting to obtain a treatment in breach of the legislation or of the provisions issued by the Company or, in any case, an unduly preferential treatment;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of committing offences of "*Bribery against the Public Administration*", in their various forms, of "*illegal inducement to give or promise benefits*" and the "*trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of contractual relations with the Company.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.3 Management of activities relating to a request for authorisation or fulfilment of requirements towards the Public Administration

This protocol applies to all the Company Structures involved in the management of activities relating to applications for authorisations or the fulfilment of requirements with the Public Administration including, by way of example and without limitation:

- management of relations with social security and social assistance entities, and performance, of labour and social security legal requirements in accordance with the established time limits and procedures (INPS – the National Social Security Agency, INAIL – the National Insurance Agency, INPDAP, Provincial Labour Office, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.) also for the purpose of managing protected categories;
- management of relations with the Chambers of Commerce for the performance of the activities relating to the Companies' Register;
- management of relations with the Local Authorities competent for waste disposal;
- management of relations with State, Regional, Municipal Administrations and Local Authorities (Local Health Authorities, Fire-fighter Service, ARPA – Regional Environmental Protection Agencies etc.) for the performance of requirements relating to health and safety and/or authorisations (for example building procedures), permits, concessions;
- management of relations with the Ministry of the Economy and Finance, with Customs and Monopolies Agencies, with Tax Agencies and with local Public Bodies for the discharge of tax obligations;
- management of relations with the Prefecture, Public Prosecutor's Office and Chambers of Commerce which issue certificates and authorisations.

Pursuant to Legislative Decree No. 231/2001, the aforementioned activities could potentially present opportunities for the commission of the offences of "bribery" in their various forms, of "Illegal inducement to give or promise benefits", of "Trafficking of illegal influences"[20] and of "Fraud against the State or other public body", of the "Smuggling crimes" and "Fraudulent transfer of valuables".

[20] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within European Community institutions, or within Entities established on the basis of the Treaties establishing the European Community, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The management of relations with the Public Administration at the time of applying for authorisations or performing legal requirements comprises the following steps:

- preparing the documents;
- submitting the required documents and keeping the file on the record;
- handling relations with the Public Bodies;
- providing assistance during visits and inspections by the Public Bodies;
- managing relations with the Public Bodies for collecting the authorisation and performing the requirements.

The operating procedures for the management of the process are governed both by the internal rules of the Company and of the Group, developed and updated by the competent Structures, which form an integral and substantive part of this protocol, and by Intesa Sanpaolo's reference regulations.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - within each Structure, the persons who intervene in the management of activities relating to the request for authorisations to the Public Administration shall be specifically identified in the Company's Organisational Manual and Functional Chart and in the internal system of powers and delegations; outside these cases, those who intervene in the process must be formally authorised and delegated by those vested with such powers and must operate exclusively within the scope of their delegation;
  - in the event that relations with public bodies are maintained by third parties, the latter are identified in a letter of assignment/appointment or in the contractual clauses;
  - relations with Public employees in the event of visits/inspections, including those performed to verify compliance with the provisions of law applicable to the activities relating to each area, shall be maintained by the Head of the structure and/or the persons specifically appointed by him/her;

- the internal organisation of delegated powers and signature powers is such as to attribute limited operational powers to the Heads of the various Corporate Structures. The charging of expenses is specifically regulated by an internal procedure, which requires, in order for the competent Structure to proceed with payment, the presentation of the supporting document for the expenses, as well as verification that the service received has actually been provided.

- Segregation of duties between the persons involved in the process of managing the activities relating to requests for authorisations or discharge of obligations towards the Public Administration (as well as in the process for managing expenses), in order to ensure that a maker and checker mechanism is in place in all phases of the process.
- Control activities: the activities must be carried out so as to ensure that the data and information accompanying the application for authorisation or supplied in performance of requirements or on request (for example bank evaluations or requests from the Finance Police concerning financial transactions) are truthful, complete, congruent and supplied in a timely manner, with specific controls in the presence of the parties concerned, where appropriate. In particular, where the authorisation/requirement includes data processing in order to prepare the documents requested by the Public Body, the correctness of the processed data shall be checked by persons different from those tasked with performing the activity.
- Process traceability including both the electronic and the paper trail:
  - copy of the documentation delivered to the public body for the request for authorization or for the fulfilment of obligations or upon request (for example bank checks and requests on financial transactions by the Finance Police), is kept in the archive of the competent structure;
  - in order to allow the reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced relating to performance of the requirements relating to applications for authorisations to the Public Administration;
  - the Head of the Structure, or another designated staff member shall sign by way of acceptance the report prepared by the Public officials at the time of performing the inspections/visits at the Company and shall keep a copy on file in his office, together with all annexes.

Rules of conduct

The Company's structures howsoever involved in the management of relations with the Public Administration relating to applications for authorisations or the performance of

requirements, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any applicable provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process who are responsible for signing papers or documents with relevance outside the Company, if not specifically indicated in the organisational manual or in the functional chart or in the system of delegations and powers, must be specifically appointed;
- staff members cannot accept any request for undue benefits or attempt at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing Function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1.
- if third parties (freelance professionals, firms etc.) are to be involved in performance of the activities relating to authorisation procedures, or to the performance of requirements towards the Public Administration, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001, the provisions of the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;
- as part of the audits carried out by Public Administration Officials at the Company's headquarters, except for situations in which the Officials request direct interviews with specifically identified Company staff, at least two persons participate in the meetings with the Officials, if belonging to the Structure involved; otherwise, where the audit is carried out by Structures other than the one involved (such as, for example: Human Resources, Organisation, Legal, Auditing and Compliance) only one person is expected to attend the meetings with the Officials.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- delay without good reason or omit the presentation of documents/communication of requested data;
- provide incomplete documentation and/or communicate false or modified data;
- use deceit which could lead Public Bodies in error;
- ask or induce (also through intermediaries) members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the response of the Public Administration;
- fictitiously attribute to others the ownership or availability of money, assets or other benefits in order to evade the law provisions on asset prevention;
- promise or pay/offer (also through intermediaries) undue sums of money, gifts or free benefits apart from courtesy gifts of low value or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration in order to further or favour the Company's interests. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons, the payment of incentives in violation of the reference rules and company regulations and, more generally, all those transactions that result in the generation of a loss for the Company and the creation of a profit for the aforementioned persons;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of committing offences of "*Bribery against the Public Administration*", in their various forms, of "*illegal inducement to give or promise benefits*" and the "*trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of relations with the Company.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.4 Management of litigation and out-of-court settlements

This protocol applies to all the Company Structures involved in the management of judicial and out-of-court litigation (administrative, civil, criminal, tax, labour and social security litigation) and out-of-court settlements with Public Bodies or private individuals.

Pursuant to Legislative Decree No. 231/2001, the relevant process could present opportunities for the commission of the offences of "*bribery*" in their various forms[21], of "*illegal inducement* to *give or promise benefits*", of "*trafficking in illegal influences*" [22] and "*fraud to the detriment of the State or other public body*", as well as the offence of "*inducing someone not to make declarations to the Judicial Authority or to make false declarations*"[23].

There is also the risk of commission of the offence of "*private-to-private corruption*" and of "*instigating private-to-private corruption*", described in Chapters 7.2 and 7.3.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

In the event of litigation, the Company, which does not have an in-house legal structure, usually avails itself of the support of the dedicated Group Structures, also through specific outsourcing contracts, or of external professionals.

The Company's internal compliance is coordinated by the competent Structure according to the subject matter of the litigation.

The process can be broken down as follows:

- opening the judicial or out-of-court litigation;
  - collecting the information and documents relating to the dispute;
  - analysing, assessing and submitting evidence;
  - drafting pleas and briefs and any supplementary documents, directly or in collaboration with the external professionals;

[21] Therein including bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code).

[22] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within European Community institutions, or within Entities established on the basis of the Treaties establishing the European Community, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

[23] This offence, punished by Article 377-bis of the Criminal Code, is a predicate offence of the liability of entities pursuant to Article 25-decies of the Decree. Moreover, pursuant to Article 10 of Law No. 146/2006 it can entail the same liability also where the offence is of transnational scope. An offence is considered to be transnational and is punished with a term of imprisonment whose maximum duration shall be of not less than four years, where it involves an organized criminal group and:

- was committed in more than one Country, or
- was committed in one Country, but a significant part of its preparation, planning, management or control took place in another Country, or
- was committed in one Country, but involved an organised criminal group which pursues criminal activities in more than one Country;
- was committed in one Country, but had a significant impact on another Country.

- managing the dispute;
- receiving, analysing and assessing the acts relating to the dispute;
- preparing case files;
- participating in the case, where useful or necessary, in the event of court proceedings;
- entertaining ongoing relations with any appointed professionals;
- adopting decisions to:
  - determine the allocations to the Provision for Risks and Charges, concerning the disputes in which the Bank is a defendant, and reporting of the event as operational risk;
  - making payments and reaching out-of-court settlements;
- closing the dispute.

The out-of-court settlement management process covers all the activities necessary to prevent or resolve a dispute through agreements or mutual renunciations and concessions, in order to avoid or close judicial proceedings. This process is normally carried out with the assistance provided by the dedicated Group Structures or by the appointed external professional and consists of the following steps:

- analysing the event which gave rise to the dispute and assessing whether there are grounds for reaching an out-of-court settlement;
- managing negotiations aimed at identifying and formalising the transaction;
- preparing, signing and implementing the out-of-court settlement.

The operating procedures for management of the process are governed by Group rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels: without prejudice to the coordination of litigation by the competent Group Structures, this is provided for within each characteristic operational stage of the process:
  - the definition of a clear attribution of powers concerning the representation of the Company before third parties before the judicial and financial administration offices and judicial bodies. Outside these cases, those who intervene in the process of settlements, representation and defence before these bodies must be identified and authorised by delegation by those with such powers;

- the engagement of external legal counsel (where no recourse is made to advice provided by the Group Structures) is authorised by the person empowered on the basis of the powers and delegations in force or by their delegate.

- Segregation of duties: by means of a clear and formalised procedure for the allocation of duties and responsibilities in performance of the activities relating to the management of disputes and out-of-court settlements, including with the Public Administration. The internal organisation of delegated powers and signature powers is such as to attribute limited operational powers to the Heads of the various Corporate Structures. The charging of expenses is specifically regulated by an internal procedure, which requires, in order for the competent Structure to proceed with payment, the presentation of the supporting document for the expenses, as well as verification by those responsible for the expense that the service received has actually been provided.
- Control activities: the internal structure of the Company competent in relation to the nature of the litigation supports the specialised Group structure or the appointed external lawyer in monitoring the progress of pending disputes; settlements relating to the litigation, ordered by the competent internal structure of the Company, are verified by the internal structure that follows the litigation together with the specialised Group structure, applying maker and checker mechanisms.
- Process traceability including both the electronic and the paper trail:
  - each relevant phase of the process must be recorded in specific written documents;
  - in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation under its competence concerning performance of procedures and activities in the management of disputes and out-of-court settlements, including with the Public Administration.

Rules of conduct

The Company Structures howsoever involved in management of disputes and out-of-court settlements, including with the Public Administration, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Code of Ethics, Internal Code of Conduct and the Anti-Corruption Guidelines of the Group.

Specifically:

- the Company's system of powers and delegations identifies the persons who are responsible for signing instruments or documents with external relevance to the

Company; those without such powers, if involved in this process, must be specifically appointed;

- if third parties are to be involved in the management of litigation and out-of-court settlement, the contracts/letters of appointment entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001, the provisions of the laws against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded, on the basis of the provisions of the relevant internal procedures; in any case, no remuneration shall be payable where it is not adequately justified by the type of work to be performed and/or the value of the dispute in relation to applicable professional fees;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing Function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1.

In any case, it is forbidden to engage in, collaborate with or induce conduct which may belong to one of the types of offences covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation, with the aim of unduly favouring the interests of the Company, also through external professionals or third parties, it is forbidden to:

- at both formal and informal meetings, or at all stages of the proceedings:
  - make any undue demand or exercise pressure upon Judges or Members of Arbitration Panels (including ancillary staff and court experts);
  - induce anyone to overstep constraints or thresholds in order to protect the Company's interests;
  - Induce, using violence or threats or, alternatively, by offering or promising money or other benefits,to induce persons to be questioned by the judicial authority and whose statements may be used in criminal proceedings to refrain from answering or to lie;
  - unduly influence the decisions of the Adjudicating Body or Public Administration positions when the latter is the adverse party in the dispute/arbitration;

- during inspections/controls/investigations, influence the judgement, opinion, report or appraisal of public bodies or bodies appointed by the Adjudicating Body or Court Police authorities;
- ask or induce – including through intermediaries – members of the Public Administration to grant preferential treatment or omit due information in order to improperly influence the management of the relationship with the Company;
- promise or pay/offer – also through intermediaries – undue sums of money, gifts or gratuitous benefits (outside the practice of courtesy gifts of modest value), or grant advantages or other benefits of any kind – directly or indirectly for oneself or for others – in favour of representatives of the Public Administration, senior officers or their staff belonging to companies that are counterparties or in relation with the Company, in order to unduly favour the interests of the Company, or threaten them with unfair harm for the same reasons. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons, the payment of incentives in violation of the reference rules and company regulations and, more generally, all those operations that result in the generation of a loss for the Company and the creation of a profit for the aforementioned persons;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines of the Group; this is in order to prevent the risk of bribery offences, in their various forms, and of "*illegal inducement to give or promise benefits*" and the "*trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Public Administration and thus the possibility of facilitating or influencing the management of the relations with the Company.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.5 Management of relations with the Supervisory Authorities

This protocol applies to all the Company Structures involved in the management of relations with the Supervisory Authorities (also through the Parent Bank) , and concerns all types of activity implemented in respect of remarks, requirements, communications, requests and inspections.

With the establishment of the SEVIF (European Financial Supervision System) in Regulations 1092, 1093, 1094 and 1095 of 2010) means that the transfer of supervisory functions at European level now takes place through:

- the Single Supervisory Mechanism (so-called SSM), which gives the ECB tasks and powers of direct, exclusive supervision of major credit institutions;
- the Single Resolution Mechanism (so-called SRM).

Pursuant to Legislative Decree No. 231/2001, the relevant process could potentially present opportunities for the commission of the offences of "*bribery*" in their various forms, of "*illegal inducement to give or promise benefits*", of "*trafficking in illegal influences*"[24] and of "*obstructing the exercise of the functions of public supervisory authorities*" (Article 2638 of the Civil Code).

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in handling relations with the Supervisory Authorities, including:

- the European Central Bank;
- the Bank of Italy;
- Consob;
- Financial Intelligence Unit (FIU);
- Data protection authority;
- the Italian Competition Authority (AGCM);
- tax supervisory authorities (the Revenue Agency).

The rules of conduct set out in this protocol shall also apply, in terms of general conduct guidelines, to relations with foreign Supervisory Authorities.

[24] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

Process description

The activities relating to the management of relations with the supervisory authorities can be broken down as follows:

- preparing/submitting occasional or periodic reports to the Supervisory Authorities;
- submitting requests/applications for approvals and/or authorisations;
- providing replies and performing requirements in response to requests/demands of the Supervisory Authorities;
- handling relations with Officials of the Supervisory Authorities during inspections;
- monitoring remediation actions and the provision of information to the supervisory authorities by providing periodic reports.

By reason of the subject/scope of communications with the Authorities, the internal structure of the Company concerned for the area of competence coordinates with the other internal structures and/or with the outsourcer, where applicable, for the management of relations and/or Supervisory authorisation procedures, as well as for the formal drafting of documents and responses in the event of inspections, consistently with the "Group Rules for the management of relations with Supervisors and Regulatory Authorities" applied by the Parent Company.

The operating procedures for the management of the process are governed both by the internal rules of the Company and of the Group, developed and updated by the competent Structures, which form an integral and substantive part of this protocol, and by Intesa Sanpaolo's reference regulations.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - with the exception of inspection visits, relations with the Supervisory Authorities are maintained by the Head of the reference Structure (on the basis of the provisions of the organisational manual and the Company functional chart or of the internal operating procedures assigning specific tasks and responsibilities), by persons specifically appointed by him by delegation, as well as by internal and external Group outsourcers on the basis of specific service agreements;
  - all deeds which involve a commitment on the part of the Company must be signed solely by duly appointed persons;
  - replies to findings raised by the authorities must, where required, be approved and/or examined by the Board of Directors.

- Segregation of duties between the persons involved in the process of managing relations with the Supervisory Authorities. Specifically:
  - the process of managing communications and reports is governed by internal procedures that define the tasks and responsibilities for preparing the documents and sending them also through outsourcers if appointed to perform such tasks;
  - with reference to the management of relations not relating to the ordinary operations of the Company's Structures, all correspondence concerning findings or exceptions relating to the Company's operations addressed to the Supervisory Authorities shall be shared in advance with the competent Compliance and AML Function;
  - with reference to audits, the Chief Executive Officer and General Manager, after ascertaining the subject of the audit, together with the Head of the Structure concerned by the audit, shall identify the resources appointed to manage relations with Public Officials during their stay at the Company. The Compliance and Internal Auditing functions, and in particularly relevant cases the Surveillance Body, must be promptly informed of the inspection in progress and of any findings or exceptions noted by the Authority.
- Specifically defined control activities:
  - checks on the completeness, correctness and accuracy of the information transmitted to the Supervisory Authorities are carried out by the Structure concerned must be supported by maker and checker mechanisms;
  - legal controls on compliance with the reference legislation applicable to the requested report/communication.
- Process traceability including both the electronic and the paper trail:
  - all the Company's structures which are howsoever involved in preparing and transmitting communications and required documents to the Supervisory authorities, must file and store the relevant documentation produced in the course of their relations with the Authority, including all documents submitted to the Authority by electronic means. This documentation must be made available at the request of the structures in charge of control activities;
  - every communication to the Supervisory Authorities concerning important data and/or information on the Company's operations shall be documented/recorded in electronic format and kept on file by the competent Structure;
  - except where the Supervisory Authority is not required to immediately issue an inspection report, the staff member of the Structure concerned who was present at the inspection shall assist the Public Official in preparing the report of the inspection and findings; the Company's staff member shall reserve the right to submit any

objections, and shall sign the inspection report prepared by the Public Official, to confirm having read the report together with all annexes;

- for every inspection made by Officials representing the Supervisory Authorities the Head of the Structure concerned shall send to other competent entities a copy of the inspection report issued by the Public Official complete with its annexes. Where no immediate issue of an inspection report by the Supervisory Authority is provided for, the Head of the Structure concerned by the inspection or the person delegated by him shall prepare a summary report of the inspection visit and shall send it to the Chief Executive Officer and General Manager and to the competent corporate Functions. Such documentation shall be kept on file by the Head of the Structure concerned by the inspection.

Rules of conduct

The Company Structures howsoever involved in the management of relations with the Supervisory Authorities shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines of the Group.

Specifically:

- the Company's system of powers and delegations identifies the persons who are responsible for signing instruments or documents with external relevance to the Company; those without such powers, if involved in this process, must be specifically appointed;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by a person of the Supervisory Authorities they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing Function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1.;
- the periodic reports to the Supervisory authorities must be submitted in a timely manner and any requests/demands from the same Authorities must be promptly acted on;
- within the scope of audits carried out by the Officials of the Authorities at the Company's registered office, except for situations in which the Officials request direct interviews with staff of the Company or of the specifically identified outsourcer, at least two persons, if belonging to the Structure involved in the inspection, shall participate in the meetings with the Officials themselves; otherwise, where the inspection is followed by Structures other than the one involved in the audit , the presence of only one person from the

Structure involved in the inspection shall be sufficient, together with another person from the Structure following the audit.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- delay without good reason or omit the presentation of documents/communication of requested data;
- present incomplete documents and data and/or communicate false or altered data;
- adopt deceitful conduct which might lead the Supervisory Authorities into error;
- ask or induce – also through intermediaries – representatives of the Supervisory Authorities to grant preferential treatment or omit due information in order to hinder performance of Supervisory duties;
- promise or pay/offer (also through intermediaries) undue sums of money, gifts or free services (outside the practices of courtesy gifts of modest value) and grant advantages or other benefits of any kind – directly or indirectly, for oneself or for others – to representatives of the Supervisory Authority with the aim of promoting or favouring the interests of the Company. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons, the payment of incentives in violation of the reference rules and company regulations and, more generally, all those operations that result in the generation of a loss for the Company and the creation of a profit for the aforementioned persons.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.6 Management of procurement procedures for goods and services and for the appointment of professional consultants

This protocol applies to all the Company Structures involved in the management of the procedures for the procurement of goods and services.

The term goods shall also include intellectual works[25], the term services shall also include all types of intellectual services (e.g. legal, fiscal, technical, labour consultancy, administrative, organisational, various forms of mediation, agency or brokering assignments, etc.), including professional or consultancy appointments, as well as assignments to third parties who, by bringing the Company into contact with potential or existing customers, promote the development of the Company's activities in the field of banking, financial and insurance services (so-called "Business Introducers[26]").

Under Legislative Decree No. 231/2001, this process could be means for the committing of offences of "*bribery*" in its various forms, or "*illegal inducement to give or promise benefits*" or "*trafficking of illegal influences*"[27].

Indeed, non-transparent process management might allow the commission of such offences, for example by creating "slush funds" after paying prices exceeding the actual value of the good/service obtained.

There is also the risk of commission of the offence of "*private-to-private corruption*" and of "*instigating private-to-private corruption*", described in Chapters 7.2 and 7.3.

The aim is also to prevent the risk of acquiring illegally obtained goods or services, and to prevent involvement in other crimes the counterparty could be exposed to (crimes against industry and trade; offences of copyright infringement; smuggling crimes, crimes of employment of illegal immigrants and illicit intermediation and exploitation of labour,[28] etc.).

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

---

[25] Pursuant to Article 2575 of the Civil Code, intellectual works protected by copyright are those belonging to the sciences, literature, music, the figurative arts, architecture, theatre, and film, irrespective of their form of expression. Computer software and data banks which by their choice of arrangement of materials constitute an intellectual work of their author are also ranked pari passu with literary works and enjoy the same protection (Article 1, Law No. 633 of 22 April 1941).

[26] Business Introducers do not include entities that carry out business development or placement of Group products/services and that are subject to specific rules or forms of supervision in their jurisdictions (e.g. Banks and other intermediaries placing investment products, Financial Advisors, Financial Activity Agents, Credit Brokers, Insurance Intermediaries).

[27] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

[28] On this point, see Chapters 7.5 and 7.9.

Process description

Management of the procedures for the purchase of goods and services includes the following processes:

- definition of the expenditure budget;
- authorisation of new expenditure and related orders;
- payment of the amounts of the expenses incurred;
- monitoring the progress of the different items of the expenditure budget;
- supplier management.

The operating procedures for management of the processes are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels:
  - pursuant to the Articles of Association, the Company's budget is prepared and approved by the Board of Directors. Furthermore, expenses strictly related to participatory investments of the fund are authorised in advance by the Board of Directors;
  - approval of the purchase request, supplier selection, conclusion of the contract and issue of the order shall be exclusively carried out by persons specifically empowered under the existing power and delegation system, which defines levels of operational autonomy by type and amount of expenditure. The internal set of rules illustrates these authorisation mechanisms, and indicates the corporate officials who hold the necessary powers. The conclusion, renewal or modification of contracts with Business Introducers must be approved by the Division Manager or an equivalent corporate structure;
  - the choice of the suppliers of goods and services and of freelance professionals is made from lists of suppliers selected on the basis of criteria identified in the internal set of rules, except for occasional needs/supplies. Suppliers must guarantee or be able to document (at the request of the Company), also with reference to the subcontractors appointed by them:
    - compliance with regulations industrial property rights and copyright and, in any case, the legitimate origin of the goods supplied and the correct completion of customs procedures (including payment of the related fees), in relation to the use of trademarks or distinctive signs and the marketing of goods or services;

        - in relation to the workers employed, compliance with immigration laws and regulations relating to pay, contributions, welfare, insurance and taxes;
    - any subcontracting of supplies of services/activities by the Company's suppliers to third parties shall be contractually conditional on prior approval by the Company structure which signed the contract;
    - the authorisation to pay the invoice is granted to the persons having the power to do so, within the limits of the authorised budget; it may be denied following a formal notice of non-compliance/shortage of supply adequately documented and detailed by the above-mentioned Structures. Remuneration of Business Introducers may be paid according to the terms, measures and conditions stipulated in the contracts, without any possibility of derogation. If the reimbursement of expenses incurred by Business Introducers is contractually agreed upon, this may only take place upon presentation of complete and clear supporting documentation of the expenses reasonably incurred;
    - the payment of invoices is verified by a specific dedicated corporate Structure on the basis of appropriate proofs of expenditure.
- Segregation of duties between the different persons involved in the procurement procedure management process. In particular: the activities relating to the different phases of the process must be carried out by different and clearly identifiable persons, and must be supported by a maker and checker mechanism.
- Control activities: the reference internal set of rules identifies the controls that must be performed by each Structure concerned in each phase of the process:
    - verification of expenditure limit and of appropriateness of the expenditure;
    - checks on the regularity, completeness, correctness and timeliness of the service provided;
    - verification of compliance with the criteria identified by the corporate regulations for the choice of suppliers and freelance professionals (the initiation of the relationship must be preceded by an adequate due diligence, as established by the Anti-Corruption Guidelines), including sample checks regarding compliance of the aforementioned guarantees concerning the authenticity and lawful origin of the goods supplied;
    - verification of compliance with legal regulations that forbid or subject to certain conditions the appointment of any kind of public employee or former public employee;

- verification of the presentation by the supplier of a guarantee or adequate documentation as to the authenticity and lawful origin of the goods supplied and the regularity of the workers employed by them;
- making the payment due following the issue of the authorisation by the person entitled to incur the expenditure and on the basis of an appropriate supporting document;
- verification of compliance with legal regulations that forbid or subject to certain conditions the appointment of any kind of public employee or former public employee.

As concerns the assignment of professional commissions and consultancies, the performance of which call for direct relationships with the Public Administration (for instance, legal expenses litigation, consultants' fees for preparing public grant applications, etc.) the Heads of the Structures concerned must:

- ensure that a list of freelance professionals/consultants, indicating the object of their commission and the consideration payable, is kept updated and available at all times;
- regularly check the above-mentioned list to identify any abnormal situations.

Relationships with Business Introducers must be governed by written contracts and provide for the Company's right to terminate them in advance in accordance with the Group Anti-corruption Guidelines. The Division Manager or an equivalent structure must keep an orderly record of the Business Introducers, indicating the volume of business procured and the remuneration paid."

- Process traceability including both the electronic and the paper trail:
  - use of IT systems supporting the operations, to ensure that the data and information relating to the procurement process are recorded and kept on file;
  - each process phase shall be documented, paying particular attention to the phase of selection of the goods and/or service supplier or the freelance professional, also through competitive bidding procedures, providing reasons for the selection and justifying the appropriateness and congruence of the price. The internal rules indicate in which cases goods and/or service suppliers or professionals must be selected by means of a competitive bidding procedure or in any event by requesting several offers;
  - in order to allow the reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced in performance of the requirements relating to management of the goods and services procurement process;

Rules of conduct

The Company Structures howsoever involved in the management of goods and service procurement procedures or in the professional commission award process shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the contractual documents governing the award of supply contracts/professional commissions must contain an ad hoc declaration that the party knows the provisions of Legislative Decree No. 231/2001, the provisions of the laws against corruption and undertakes to comply with them;
- the payment of fees or compensation to any external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed;
- the payments shall be made only into a current account held by the supplier/freelance consultant with whom the relationship has been established;
- payments in cash, payments to a country other than the one in which the counterparty is established or to a party other than the latter shall not be allowed.

In any case, it is forbidden to engage in, collaborate with or induce conduct which may be instrumental to commission of one of the types of offences covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- award goods/services supply contracts and professional commissions where no expenditure authorisation has been issued, or where the necessary requirements of professionalism, quality and cost-effectiveness of the goods or services supplied are not met;
- attest to the regularity of the goods/services upon receiving them, without having carefully assessed their actual quality and congruence;
- authorise the payment of goods/services without having checked that they match contract terms and specifications;
- authorise the payment of professionals' fees without having carefully checked the amount of such fees against the quality of the service received;

- make payments to the Company's suppliers that are not adequately justified in the context of the existing contractual relationship with them or in the absence of adequate justification;
- threaten suppliers with retaliation if they provide services to or use the services of competitors of the Company;
- introduce goods that violate the provisions, prohibitions and limitations set out in the Consolidated Law on customs;
- promise or pay/offer (also through intermediaries) undue sums of money, gifts, free benefits (outside the scope of practices regarding courtesy gifts of little value), and grant advantages or other benefits of any kind – directly or indirectly for oneself or for others – in favour of exponents/representatives of the Public Administration and/or senior officers or their staff belonging to companies that are counterparts or in relation with the Company, in order to further or favour the interests of the Company, or threaten them with unfair harm for the same reasons. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons, the payment of incentives in violation of the reference rules and company regulations and, more generally, all those operations that result in the generation of a loss for the Company and the creation of a profit for the aforementioned persons.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.7 Management of gifts, entertainment expenses, donations to charities and sponsorships

This protocol applies to all the Company Structures involved in the management of gifts, entertainment expenses, donations to charities and sponsorships.

For the purposes of this protocol, the following definitions shall apply:

- gifts[29] means goods having a low value which are offered at no charge, in the framework of normal business relations, in order to promote the Company's business;
- entertainment expenses means the expenses incurred by the Company in pursuing commercial relations, for the purpose of promoting and improving the Company's image (for example: costs for lunches and refreshments, expenses for welcome and hospitality activities, etc.);
- charitable contributions means money donations which the Company makes exclusively to non-profit organisations;
- sponsorships means the promotion, enhancement and strengthening of the Company's image by concluding atypical agreements (free-form agreements, asset agreements, mutual services agreements) with external organisations (e.g.: sports clubs associations, including amateur associations, non-profit organisations, local agencies and local bodies, etc.).

Under Legislative Decree No. 231/2001, this process could be means for the committing of offences of "*bribery*" in its various forms, or "*illegal inducement to give or promise benefits"*, or "*trafficking of illegal influences*"[30].

There is also the risk of commission of the offence of "*private-to-private corruption*" and of "*instigating private-to-private corruption*", described in Chapters 7.2 and 7.3.

This is because non-transparent management of the processes relating to gifts, entertainment expenses, donations to charities and sponsorships could enable the commission of such offences, for example by giving/granting advantages to members of the Public Administration and/or senior officers and/or their staff in companies or entities that are counterparties or in relationships with the Company in order to favour the Company's interests or by creating funds that can be used to commit such offences.

[29] Under no circumstances may gifts consist of sums of money.

[30] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within EU institutions, or within Entities established on the basis of the Treaties establishing the EU, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The processes relating to management of gifts and entertainment expenses concern goods or services intended to be freely given for commercial courtesy purposes to third parties, such as, for example, customers, suppliers, Public Administration Bodies, public institutions or other organisations.

Gifts or other types of presents (such as invitations to sports events, shows and entertainment, tickets, etc.) which originate from or are provided to the same individual/entity which do not exceed the value of Euro 150 in one calendar year are considered to be acts of commercial and/or institutional courtesy of a moderate value.

With regard to the management of gifts and sponsorships in particular, the company makes use of the parent company on the basis of a specific service contract.

The above-mentioned processes are structured on the basis of the operating rules laid down in the internal rules on expenditure and in the protocol *"Management of the procedures for the procurement of goods and services and for the appointment of professional consultants"*, which provide for the following operational steps:

- definition of the expenditure budget;
- authorisation of new expenditure and management of related orders in the cases provided for;
- payment of the amounts of the expenses incurred;
- monitoring the progress of the different items of the expenditure budget.

The operating procedures for the management of the processes are governed both by the internal rules of the Company, developed and updated by the competent Structures, which form an integral and substantive part of this protocol, and by Intesa Sanpaolo's reference regulations for the activities outsourced to it.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels:
  - expenditure on gifts and entertainment may only be authorised by corporate bodies with the necessary powers, clearly identified in the internal rules;
  - gifts or other presents that exceed the value of Euro 150 may be allowed, on an exceptional basis, in consideration of the profile of the donor or the beneficiary as

well as the nature of the gift itself[31] and in any case within the limits of reasonableness, subject to authorisation by the corporate bodies endowed with the necessary powers. The limits set on the amounts on an annual basis for the gifts and other presence do not apply to entertainment expenses relative to events and forms of hospitality (including lunch and dinner) with the participation of corporate representatives and Company personnel, provided they are strictly related to the business or institutional relationship and reasonable as compared to the commonly accepted practices of commercial and/or institutional courtesy;

- recourse to the banking Parent Company is made in accordance with the existing service contract.

- Segregation of duties: between the different persons involved in the processes. In particular: the activities relating to the different phases of the process must be carried out by different and clearly identifiable parties/persons, and must be supported by a maker and checker mechanism.
- Control activities:
  - the internal set of rules also defines the procedures according to which the disbursement of donations to charities (including cases of membership of foundations, associations and other non-profit organisations with the intention of donation, involving the disbursement of funds or future commitments in this respect) and sponsorships must be preceded by a due diligence process, particularly insofar as the provisions set forth in the Anti-Corruption Guidelines are concerned to be carried out by the Structure involved. In particular, the analysis and verification of the type of organisation and of its statutory objects is required;
  - the analysis and verification of the type of organisation and of its statutory objects is required;
  - the verification and approval of all disbursements by the Head of the Structure concerned;
  - the verification that total disbursements are established annually and funded from a specific budget approved by the competent Bodies;
  - with regard to sponsorships, proper performance of the agreed service by the sponsored entity shall be verified, by acquiring appropriate documentary evidence of such performance.

  Furthermore, the Heads of the Structures concerned must:

[31] Reference is made, by way of example, to situations in which gifts are components of offers with a predominantly professional content, such as invitations to conferences and seminars.

- ensure that the list of beneficiaries is kept updated and available at all times, including the value of the disbursements or of the gifts distributed, and the dates/occasions of the donations. This requirement does not apply to “branded” gifts, i.e. those bearing the Company’s logo (such as pens, desk items, etc.), and the standard gifts (for example, for the end of the year);
- regularly check the above-mentioned list to identify any abnormal situations.

- Process traceability including both the electronic and the paper trail:
  - complete traceability, at document and system level, of the management processes of gifts, entertainment expenses, charities and sponsorships, including any expenditure incurred in that capacity, in order to allow the reconstruction of the responsibilities and reasons for the choices made;
  - within the process, the persons involved must be clearly identifiable; moreover, accounting and payment activities must be carried out by persons other than those who authorise the incurrence of expenses.

Rules of conduct

While expenses for gifts are allowed, provided they are of limited value and, in any case, not such as to compromise the integrity and reputation of either of the parties and not such as to influence the beneficiary’s independent judgement, the Company’s structures, howsoever involved in the management of gifts, entertainment expenses, donations to charities and sponsorships are required to comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group’s Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines. Specifically:

- the Company may make disbursements in the form of donations to charities or sponsorships to support the initiatives of lawfully established Entities whose activities are not in conflict with the Company's and the Group’s ethical principles and, in the case of donations for charity, these entities cannot operate on a for profit basis;
- any initiatives falling under one of the categories eligible for “sponsorships” cannot at the same time benefit from charitable contributions;
- in the case of charitable donations and sponsorships, the beneficiary body is required to issue a declaration of awareness of the legal provisions against corruption and a commitment to comply with them;
- the donations shall be paid into a current account held by the beneficiary entity exclusively; payment in cash or payments to a country other than that of the beneficiary entity or to an individual /entity other than the latter are not allowed.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- make donations, for charitable or sponsorship initiatives, to Entities involved in notorious judicial cases, practices that are not respectful of human rights or contrary to vivisection and environmental protection regulations. No charitable contributions or sponsorships may be given to political parties and movements and their subsidiary organisations, trade unions and welfare associations (*patronati*), clubs (e.g. Lions, Rotary, etc.), recreational associations and groups, private schools, private schools legally equivalent to public schools and/or legally recognised schools, except for particular initiatives of special social, cultural or scientific value must be approved by the Corporate Anti-Corruption Officer;
- make donations/gifts to Entities/members/representatives of the Public Administration, Supervisory Authorities or other public institutions or to other organisations/persons linked to such bodies thereby infringing this protocol and the Anti-Corruption Guidelines;
- promise or pay/offer (also through intermediaries) undue sums of money, gifts, services free of charge (outside the accepted practices of courtesy gifts of little value) or grant advantages or other benefits of any kind – directly or indirectly, for oneself or for others – to members/representatives of the Public Administration, Supervisory Authorities or other public institution or to other organisations in order to further or favour the Company's interests, also yielding to unlawful pressures. Staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report it for appropriate action to their direct superior, who in turn forwards the report received to the Internal Auditing Function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- promise of pay/offer undue sums of money, gifts, services free of charge (outside the accepted practices of courtesy gifts of little value) and grant advantages or other benefits of any nature – directly or indirectly, for oneself or for others – in favour of senior officers or their staff in companies that are counterparties or in relationships with the Company, in order to unduly favour the interests of the Company;
- make a gift of goods whose lawful origin has not been verified nor their compliance with the provisions on intellectual property rights, trademark and industrial property right in general and geographic indications and protected designations of origin.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.8 Management of the staff selection and recruitment process

This protocol applies to all the Company Structures involved in the management of the staff selection and recruitment process.

The process could constitute one of the instrumental ways through which the crimes of "*bribery*" in their various types, of "*illegal inducement to give or promise benefits*", of "*trafficking in illegal influences*"[32], as well as the offences of "*bribery*among private individuals" and "*incitement to bribery among private individuals*" (described in Chapters 7. 2 and 7.3.).

This because non-transparent management of the staff selection and recruitment process could allow the commission of such offences through the promise of hiring made to representatives of the Public Administration and/or senior officers and/or their staff in companies or entities that are counterparties or in relationships with the Company, or to persons indicated by them, in order to influence their independence of judgement or to ensure any benefit for the Company.

There is also the risk of commission of the offence of the "*Employment of foreign nationals with irregular permits of stay*".

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The Company uses the outsourcer Intesa Sanpaolo to carry out its personnel selection and recruitment activities.

The staff selection and hiring process comprises the following steps:

- Staff selection:
  - needs analysis and request for new hirings;
  - identification of the required candidate profile;
  - search within the Group for staff to fill a certain position;
  - in the event of unsuccessful recruitment of candidates from outside the Group;
  - candidate selection;
  - choice of the candidates to be hired;
  - requesting authorisation from the Parent Company.
- Formalisation of hiring.

[32] As already stated, under Article 322-bis of the Criminal Code, the conduct of the bribe-giver, instigator or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within European Community institutions, or within Entities established on the basis of the Treaties establishing the European Community, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

TheCompany Structures so empowered shall directly handle the selection and hiring process concerning specialised and highly qualified staff or top managers (direct hiring).

The operating procedures for the management of the process are mainly regulated in the reference regulations of Intesa Sanpaolo, outsourcer for the activities in question.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Expressly defined authorisation levels:
  - the staff selection and recruitment process is centrally managed by the competent Structure which receives formal requests for the hiring of new staff from the Structures concerned and assesses them consistently with the budget and internal development plans;
  - recruitment authorisation granted by the Board of Directors; the Board of Directors also appoints the members of the Company's Investment Teams and, if provided for in the Fund's Management Rules, the Keymen in accordance with the procedures specifically identified in the managed Fund Regulations;
  - recruitment of candidates identified as suitable following the issue of authorisation by the competent structure of the parent company on the basis of the current system of powers and delegations.
- Segregation of duties between the different persons involved in the process. In particular, the final approval of the hiring is entrusted to the aforementioned Corporate Bodies, and is subject to the granting of consent by the Parent Bank.
- Control activities:
  - during the selection process, each candidate has to fill specific forms, to ensure that the candidates' details are collected in a uniform manner;
  - the actual hiring must be preceded by adequate due diligence particularly with regard to the provisions of the Anti-Corruption Guidelines.
- Process traceability including both the electronic and the paper trail:
  - in order to allow reconstruction of responsibilities and the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produced (including standard documents such as tests, application forms, employment contracts, etc.) relating to performance of the requirements in the course of the staff selection and hiring process.

Rules of conduct

The Company's structures howsoever involved in management of the staff selection and hiring process, shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and relevant provisions of the Code of Ethics, the Group's Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Public Administration they might receive or simply become aware of, and must immediately report it for appropriate action to their direct superior, who in turn forwards the report received to the Internal Auditing Function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- the selection must be made from a shortlist of candidates, except in the case of specialised, qualified staff that is included in protected categories or individuals to be hired for managerial positions;
- the comparative assessment of the candidates must take place on the basis of the criteria of skill, professionalism and experience in relation to the position in question;
- if the hiring process concerns:
  - disabled staff, the recruitment of candidates is arranged from lists of persons in protected categories to be requested from the relevant Employment Office;
  - foreign workers, the process must guarantee compliance with the immigration laws of the country in which the recruiting organisational unit is based and verification of possession of residence permits, where applicable, for the entire duration of the employment contract;
  - former public employees, the process must guarantee compliance with legal restrictions.
- if third parties are to be involved in the management of the staff selection and hiring process, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001, the provisions of the law against corruption and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants who may be involved in the staff selection and recruitment process is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- promise to hire (also through intermediaries), or accede to requests to hire representatives/members of the Public Administration or persons indicated by them, in order to influence their independence of judgement or to induce them to grant the Company any advantages;
- promise to hire, or accede to requests to hire senior officers or their staff in companies that are counterparties or in relationships with the Company or persons indicated by them, in order to unduly favour the pursuit of the Company's interests.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.2.2.9 Management of relations with regulatory bodies

This protocol applies to all the Structures involved in the management of relations with the Supervisory Authorities with the power to produce regulations relevant to the Company, and concerns all types of activity implemented in respect of remarks, requirements, communications, requests and inspections. This also includes advocacy services or the preparation of opinions, proposals and replies to consultations on regulations already existing, or about to be introduced. Refer to protocol 7.2.2.5. with regard to relations with the Supervisors.

Pursuant to Legislative Decree No. 231/2001, this process could present opportunities for committing the offences of "*Bribery*" in its various forms, of "Illegal inducement to provide or promise benefits", and "*Trafficking of illegal influences*"[33].

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the management of relations with:

- all Italian and international institutions, including but not limited to the Italian parliament, local governments, the Government, the Bank of Italy, the AGCM, the OAM, the OCF, CONSOB and the Data Protection Authority, foreign governments or parliaments, regulatory bodies in countries which are relevant to the activities of the Company;
- all international and multilateral institutions, including but not limited to EC institutions (the European Commission, the Council of the European Union and the European Parliament), the European Supervisory Authorities ("ESAs"), the European Central Bank, the European Data Protection Board ("EDPB"), the Basel Committee for Banking Supervision ("BCBS"), the Financial Stability Board ("FSB"), the World Bank ("WB") and the International Monetary Fund ("IMF");
- the trade associations, think tanks and interest groups in which the Company participates with or without permanent representatives, in order to set up – in line with the principles on the safeguarding of competition – discussion groups with other market players or stakeholders of the Company for the preparation of opinions, proposals or replies to consultations on existing or future regulations.

[33] As already stated, under Article 322-*bis* of the Criminal Code, the conduct of the bribe-giver or person accepting illegal inducement is a punishable criminal offence not only when it involves Public Officials and Public Service Providers within the Italian Public Administration, but also when it involves: i) persons holding corresponding functions or performing corresponding activities within European Community institutions, or within Entities established on the basis of the Treaties establishing the European Community, or, lastly, within the other European Union Member States; ii) individuals performing corresponding functions or activities in other foreign states, international or supranational public organisations, international parliamentary assemblies or international courts.

Process description

Activities relating to the management of relations with the supervisory authorities, either directly or through third parties (consultants, trade associations, think tanks and interest groups) are as follows:

- contact with the Entity;
- compliance with specific requests/consultation documents;
- the production of specific demands or position papers.

Depending on the subject/scope of the individual contact or the individual issue, the relevant Structure of the Company shall coordinate with the other internal structures and/or with the outsourcer, where applicable, for specific aspects and contributions for the areas of competence identified from time to time, consistently with the "Group Rules for the Management of Relations with Supervisors and Regulatory Authorities" adopted by the Parent Company.

The operating procedures for the management of the process are governed both by the internal rules of the Company, developed and updated by the competent Structures, which form an integral and substantive part of this protocol, and by Intesa Sanpaolo's reference regulations.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Expressly defined authorisation levels. Specifically:
  - relations with Supervisory Authorities are maintained by the Head of the reference Structure (on the basis of the provisions of the organisational manual and of the Company functional chart or of the internal operating procedures assigning specific tasks and responsibilities), by persons specifically appointed by him/her by means of proxy, to be kept by the Structure itself;
  - all instruments which involve a contractual commitment on the part of the Company must be signed solely by duly appointed persons.
- Control activities:
  - controls concerning the completeness, correctness and accuracy of the information provided to the Supervisory Authorities by the Structure concerned as to the activities falling under its competence that must be supported by maker and checker mechanisms;
  - verification of compliance with the criteria laid down in company regulations regarding the selection of suppliers and professionals (before the relationship is

established, due diligence must be carried out with particular regard to the requirements of the Anti-corruption Guidelines).

- Process traceability including both the electronic and the paper trail:
  - each key phase of the process must be recorded in writing;
  - to enable a clear understanding of the responsibilities and the motives behind the choices made, the Structure from time to time involved shall be responsible for archiving and preserving the documentation produced also by electronic means, in relation to the management of relations with regulatory bodies.

Rules of conduct

The Company Structures howsoever involved in the management of relations with the Supervisory Authorities shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

Specifically:

- the persons involved in the process that are responsible for signing acts or documents which are relevant outside the Company must be expressly appointed;
- staff members cannot accept any request for undue benefits or attempts at extortion in office by an official of the Supervisory Authorities, and more generally of the Public Administration, they might receive or simply become aware of, and must immediately report any such cases to their direct superior, who in turn forwards the report received to the Internal Auditing function and Corporate Anti-Corruption Officer for assessment and the completion of any formalities to the Surveillance Body in accordance with the provisions under Chapter 4.1;
- staff must provide the Supervisory Authorities with accurate, truthful, correct and up-to-date information, and must differentiate facts from opinions; they must not present information in a way that could give rise, even potentially, to confusion, misunderstanding or error on their part;
- staff must unequivocally declare any existing or potential conflict of interest in advance, to the Authorities;
- if third parties are to be involved in the handling of relations with the regulators or with the public administration in general, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001 and undertake to comply with them;
- the payment of fees or remuneration to any service providers involved is subject to prior authorisation to be issued by the Structure which is competent to assess the quality of service and the consequent appropriateness of the remuneration requested; in any

case, no remuneration shall be payable to service providers where it is not adequately justified by the type of work performed or to be performed.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- ask or induce representatives of the Supervisory Authorities or the Public Administration in general to grant preferential treatment;
- promise or pay/offer (including through intermediaries) undue sums of money, gifts or free benefits (apart from courtesy gifts of low value) or grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Supervisory Authorities or of the Public Administration in order to further or favour the Company's interests. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons and, more generally, all those operations that result in the generation of a loss for the Company and the creation of a profit for the aforementioned;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines; this is in order to prevent the risk of committing offences of "*Bribery against the Public Administration*", in their various forms, and of the offence of "*Illegal inducement*" offences or of "*Trafficking of illegal influences*", which could result from the selection of individuals who are "close" to persons linked to the Supervisory Authorities or to the Public Administration and thus give rise to the possibility of facilitating or influencing the management of contractual relations with the Company.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.3 Sensitive area concerning corporate offences

7.3.1 Type of offence

Article*25-ter* of the Decree covers almost all the corporate offences set forth in Title XI of Book V of the Civil Code or in other special laws, which can be qualified as general offences, since they are not specifically referable to the exercise of the specific financial activities typical of the Company[34].

The corporate offences considered concern various areas, and relate in particular to the preparation of the financial statements, external communications, certain capital or corporate transactions, obstructing controls and hindering the performance of supervisory functions. All these types of offences have been defined for the common purpose of ensuring transparency of accounting documents and corporate management and the provision of sound information to shareholders, third parties and the market in general.

With regard to the types of criminal offences in respect of accounting documents and the controls to be performed by the Supervisory Authorities, it should be noted that the Company is well placed to put in place effective prevention measures to soundly implement legislative provisions, as it is governed by special legislation requiring it to adopt a specific procedure for preparing accounting reports, and it must fulfil a series of obligations and requirements towards the Authorities. As a consequence, the procedures for managing the risk of offences outlined in this document reflect actions which are already well established in practice, or which derive in any way from the application of the primary legislation and regulation in force.

The types of offences cited by Article 25-*ter* of the Decree are listed below.

False corporate reporting (Article 2621 of the Civil Code)

False corporate reporting by listed companies (Article 2622 of the Civil Code)

These offences are committed by conduct which, with reference to the view of the profit and loss, balance sheet or cash flow situation of the Company or of the Group it belongs to, consist in the knowledgeable:

- presentation of untrue material facts in the financial statements, reports or other corporate disclosures addressed to the shareholders or the general public;
- omission of relevant material facts whose disclosure is required by the law.

[34] Article*25-ter* was amended by:

- Law No. 190/12 that added the reference of the new offence of "*Private-to-private corruption*" envisaged in Article 2635, paragraph 3, of the Civil Code, which entered into force on 28 November 2012;
- Law No. 69/15, that eliminated references to conditions for liability of legal Entities partially different from the ordinary conditions for corporate crimes and reformed the offences of "*False corporate reporting*" with effect from 14 June 2015.

In any case, the conduct is a punishable offence when it is carried out for the purpose of unfair gain for the perpetrators or others and is capable of actually leading the intended recipients to err. Furthermore, the illegal act subsists even if it refers to assets held or administered by the company on behalf of third parties.

When the false reporting concerns unlisted companies or those deemed equivalent thereto[35]:

- the presentation of untrue material facts constitutes the offence in question only if it is contained in corporate communications required by law and if the facts are relevant;
- reduced penalties and the grounds for exclusion of liability to criminal punishment applies in particularly exiguous cases[36].

False reports or communications from the independent auditors (Article 27 of Legislative Decree No. 39/2010)

The offence occurs where the persons in charge of the auditing process make false statements or conceal information on the profit and loss, balance sheet or cash flow situation of the audited company, in order to obtain an unfair gain for themselves or others, with full awareness of the falsity of the statements and with the intention of deceiving the recipients of the communications.

This offence is punished more severely where: it causes financial damage to the recipients of the communications; it concerns the auditing of certain entities defined by the Decree as being “of public interest” (including listed companies, the issuers of financial instruments having wide public circulation, banks, certain insurance companies, stock brokerage companies (SIM), asset management companies (SGR), UCITs, the financial intermediaries referred to in Article 107 of the Consolidated Banking Act); it is committed in exchange for money or other benefit; it is committed in conspiracy with members of the audited company.

The main offenders in this type of crime are the heads of the independent auditors (offence connected to their office). Also envisaged is the punishment of any person who gives or promises money or benefits, and to the general managers and the members of the administrative organ and of the control body of the public interest entities who aid and abet in commission of the offence.

[35] Deemed equivalent to companies listed in a regulated national or European Union market are the companies that control them, companies that are issuers of financial instruments for which admission to trading in said markets has been requested or that are traded on an Italian multilateral trading facility, as well as companies that make public offering transactions, or in any case which manage them.
[36] See Article 2621-*bis* of the Italian Civil Code which provides for a smaller penalty if the facts are of minor entity, in consideration of the nature and size of the company and of the methods or effects of the conduct, or if the facts regard small companies that cannot be subject to bankruptcy proceedings. In the latter case, the offence is prosecutable only through lawsuit. Additionally, Article 2621-ter of the Italian Civil Code cites the enforceability of Article 131-bis of the Criminal Code that excludes liability to punishment when, due to the methods of the conduct and to the exiguity of the damage, or of the hazard, the offence is particularly exiguous and the conduct is not habitual.

At present, this does not constitute an offence in which corporate administrative liability is presumed[37].

Obstruction of controls (Article 2625 paragraph 2 of the Civil Code)

The offence referred to in Article 2625 paragraph 2 of the Civil Code occurs where the directors conceal documents or otherwise act so as to prevent or hinder performance of the control activities legally vested in the shareholders or other Corporate bodies, thereby causing damage to the shareholders. The offence is prosecutable on the complaint of the injured party, and the sentence shall be harsher if the offence involves a listed company or issuers whose financial instruments are widely circulated among the public.

The case of obstruction of control of an independent auditor, originally also envisaged in Article 2625 of the Civil Code[38], at present does not constitute an offence in which corporate liability is presumed.

Undue repayment of contributions (Article 2626 of the Civil Code)

In its typical form, this offence, apart from cases of lawful share capital reductions, occurs where the shareholders' contributions are returned to them, also by means of simulated transactions, or where the shareholders are exempted from the obligation to make such contributions.

Unlawful distribution of profits and reserves (Article 2627 of the Civil Code)

This offence consists of distributing profits or advances on profits not actually made, or which under the law should be appropriated to reserves, or of distributing reserves, including those not created through profits, which are legally non-distributable.

It should be noted that returning the profits or re-establishing the reserves before the time-limit specified for approval of the financial statements extinguishes the offence.

---

[37] Article 25-ter of Legislative Decree No. 231/2001 even now refers to Article 2624 of the Civil Code which originally envisaged this offence, despite regulatory developments in the meantime. Indeed:

- Law No. 262/2005 introduced Article 174-bis of the Finance Consolidation Act, which used a separate instance to punish the inclusion of false information in the audit of listed companies, their subsidiaries and issuers whose financial instruments are widely circulated among the public;
- after reform of statutory auditing regulations, both Article 2624 of the Civil Code and Article 174-bis of the Finance Consolidation Act were repealed and, with effect from 7.4.2010, giving false information in audits is punished under the new terms envisaged in Article 27 of Legislative Decree No. 39/2010.

This development gave rise to serious doubts about the permanent qualification of corporate liability for such conduct. By judgement 34476/2011, the Joint Criminal Chambers of the Court of Cassation decided that the offence of giving false information in statutory audits now envisaged in Article 27 of Legislative Decree No. 39/2010 no longer falls within the scope of application of corporate administrative liability, in that this ruling is not referred to in Article 25-ter of Legislative Decree No. 231/2001. It should also be considered that certain bribes in relation to auditors are envisaged and punished pursuant to Articles 28 and 30 of Legislative Decree No. 39/2010, but do not constitute an offence for which corporate liability is presumed.

[38] Article 2625 of the Civil Code also contemplated the offence of obstruction of control of directors in relation to independent auditors. Following the reforms to the rules on the legal auditing of accounts, this offence is no longer governed by Article 2625 civil code. It was reformulated within Article 29 of Legislative Decree No. 39/10 and was then decriminalised in Legislative Decree No. 8/16; As Article 25-ter of Legislative Decree No. 231/2001 was not amended to include a reference to Article 29, it can be said that the offence of impeding the work of the auditing firm is no longer covered by the rules on corporate administrative liability. In this respect the principle indicated in the Court of Cassation judgement referred to in the previous note would seem to apply.

Unlawful dealing in the stocks or shares of the company or its parent company (Article 2628 of the Civil Code)

This offence is committed by the purchase or the subscription, apart from the cases permitted by law, of stocks or shares in the company itself or in its parent company, which cause damage to the integrity of the share capital or of non-distributable reserves.

It should be noted that if the share capital or the reserves are restored before the time limit for approval of the financial statements for the period in which the event took place the offence is extinguished.

Transactions prejudicial to creditors (Article 2629 of the Civil Code)

This offence is committed when, in breach of the provisions of the law protecting creditors, reductions in share capital or mergers with other companies or demergers are carried out, such as to cause damage to the creditors.

It should be noted that compensating the creditors for the damage incurred before the judgement is a means of extinguishing the offence.

Failure to disclose conflicts of interest (Article 2629-bis of the Civil Code)

This offence occurs where a director of a company listed on an Italian or EU regulated market or whose shares are widely distributed among the public, or of a company subject to supervision pursuant to the Banking Law, the Consolidated Law on Financial Intermediation or to legislation on insurance activities or supplemental pension funds fails to notify, in the manner and within the deadline set out in Article 2391 of the Civil Code the body he belongs to or the company and in any case the Board of Statutory Auditors, of any interest they might have personally or on behalf of third parties in a given transaction of the company in question, or, in the case of Chief Executive Officer, he does not abstain from carrying out this transaction, thereby causing a damage to the company or to third parties.

Fictitious capital formation (Article 2632 of the Civil Code)

This offence takes place where the directors and shareholders making capital contributions falsely form or increase the company's capital by assigning a number of stocks or shares for an overall value exceeding the amount of the share capital, by mutual underwriting of stocks or shares, by substantially overvaluing contributions made in kind or through receivables or by overvaluing the company's assets in the event of company transformation.

Improper distribution of the company's assets by its liquidators (Article 2633 of the Civil Code)

The offence occurs where the liquidators distribute the company's assets among the shareholders before paying off the company's creditors or before appropriating the sums necessary to satisfy creditors' claims, thereby causing damage to the creditors.

It should be noted that compensating the creditors for the damage incurred before the judgement is a means of extinguishing the offence.

Private-to-private corruption (Article 2635, paragraphs 1 and 3, of the Civil Code). Instigating private-to-private corruption (Article 2635 bis, paragraph 1 of the Civil Code).

The offence of "*private-to-private corruption*" is any act by the directors, general managers, financial reporting officers, statutory auditors, liquidators or other individuals vested with powers of management within a company or private entity and persons subject to their management or supervision, who – either directly or through another person, for themselves or for others – solicit or receive cash or other undue benefits, or accept the promise of cash or benefits in order to carry out or omit an act that conflicts with their duties or with their obligations of loyalty towards their company or private entity.

The conduct of the bribe-giver is also punished. This is the person who improperly offers, promises or gives money or other gifts, including through another person.

Punishment for *"instigating private-to-private corruption"* falls on the person that makes an offer or promise that is not accepted, or the managers of companies or private entities that solicit the gift or promise are punished, if their solicitation is not accepted[39].

Only the conduct of the bribe-giver (offer, gift or promise, whether or not they are accepted), not that of the bribe-takers (acceptance or solicitation), constitute an offence of administrative responsibility, if the offence is committed in the interest of the entity the bribe-giver belongs to[40].

Both these offences are automatically subject to prosecution.

Unlawfully influencing the shareholders' meeting (Article 2636 of the Civil Code)

Persons who obtain a majority in the shareholders' meeting by simulation or fraud, in order to achieve an unfair profit for themselves or for others are punished with incarceration.

Market rigging (Article 2637 of the Civil Code)

[39] The crime of instigating bribery exists only if the offer or promise are made to, or the solicitation is formulated by directors, general managers, managers responsible for preparing the company's financial reports, statutory auditors or liquidators or other individuals vested with powers of management within a company or private entity. The same offence committed by/directed to employees who do not perform managerial functions does not constitute incitement.

[40] The reform of the crime of "private-to-private corruption" and of "instigating private-to-private corruption" was provided for in Legislative Decree No. 38/2017, which is in effect from 14 April 2017. Actions committed prior to that date were considered bribery among individuals only if the conduct actually constituted an action that was contrary to the duties and caused damage to the company the bribe-givers belonged to, and did not apply if the actions were against private entities that were not incorporated. The addition of private entities appears to be comprehensive and is not limited to associations and foundations with a legal personality.

This offence refers to the spreading false information or setting up simulated transactions or the use of other devices likely to significantly alter the price of financial instruments which are not listed and for which no application for listing on a regulated market has been made, or likely to have a significant impact on public confidence in the financial stability of the Company or of the group to which it belongs.

For conduct that refers to issuers of listed instruments or instruments for which a request has been made for listing on a regulated market, the market abuse sanctions and connected administrative liability continue to apply.

Obstruction of the duties of the Public Supervisory Authorities (Article 2638 of the Civil Code)

This offence occurs when submitting mandatory communications to the public supervisory authorities, if untrue material facts are declared, albeit the subject of estimates, or facts that should have been reported are totally or partially concealed by fraudulent means, concerning the company's profit and loss, balance sheet or cash flow situation, for the specific purpose of obstructing the Supervisory Authority's activity.

This offence is also generated by any active or omissive conduct having the effect of hindering performance of the Supervisory Authorities' duties.

The penalty is increased if the offence involves a listed company or issuers whose financial instruments are widely distributed among the public.

False statements in prospectuses (Article 173-bis of Legislative Decree No. 58/1998)

The new Article 173-*bis* of Legislative Decree No. 58/1998 punishes the conduct of any person who includes false information or conceals data or news in the prospectuses required for public offerings or for admission to trading on regulated markets, or in the documents required for public purchase or exchange offers.

For this conduct to constitute an offence, the person engaging in it must act with the intention of deceiving the recipients of the prospectuses, in order to obtain an unfair profit for himself or others. Moreover, the false or omitted information must be such as to lead their recipients into error.

At present, this does not constitute an offence in which corporate administrative liability is presumed[41].

[41] Article 25-*ter* of Legislative Decree No. 231/2001 even now makes no reference to Article 2623 of the Civil Code, which originally envisaged this offence. Law No. 262/2005 repealed the regulation and introduced the current offence of false statements in prospectuses pursuant to Article 173-bis of Legislative Decree No. 58/1998. As Article 25-ter was not subsequently amended, this seems to confirm that the offence of false statements in prospectuses does not constitute an offence in which corporate administrative liability is presumed. In this respect the principle indicated in the Court of Cassation judgement referred to previously would seem to apply.

.

False or omitted statements for the issuance of the preliminary certificate (Article 54 of Legislative Decree No. 19/2023)

Article 54 of Legislative Decree No. 19/2023 punishes the conduct of any person who, in a cross-border merger transaction, in order to make it appear that the conditions for the issuance of the preliminary certificate have been fulfilled, draws up wholly or partly false documents, alters true documents, makes false statements or omits relevant information.

The preliminary certificate is issued by the notary who does so at the request of the Italian company taking part in the merger after verifying the proper fulfilment of the acts and formalities preliminary to the execution of the corporate transaction.

7.3.2 Sensitive company activities

The sensitive activities identified by Model which involve the highest risks of corporate offences are the following:

- Management of relations with the Board of Statutory Auditors and the Auditing Company;
- Management of periodic reporting;
- Purchase, management and disposal of investments and other assets;
- Management of relations with Supervisory Authorities.

Below, for the first three sensitive activities listed above, are the protocols setting out the principles of control and conduct applicable to these activities, which are supplemented by detailed company regulations governing them. With reference to private-to-private corruption in particular, this crime can have a potential far-reaching impact that affects all Company activities, so reference is also made to the sensitive activities contemplated in the following protocols, as they contain principles for the effective prevention of this crime:

- Management of disputes and out-of-court settlements (Chapter 7.2.2.4);
- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants (Chapter 7.2.2.6);
- Management of gifts, entertainment expenses, donations to charities and sponsorships (Chapter 7.2.2.7);
- Management of the staff selection and recruitment procedures (Chapter 7.2.2.8);

Finally, with regard to the activity indicated under the point "Management of relations with the Supervisory Authorities", please refer to the protocol referred to in Chapter 7.2.2.5, having the specific purpose of preventing, in addition to the offence of "*Bribery against the Public Administration"*, also the corporate offence referred to in Article 2638 of the Civil Code.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.3.2.1 Management of relations with the Board of Statutory Auditors and the Independent Auditors

This protocol applies to the members of the Board of Directors and to all the Bodies and Structures of the Company involved in the management of relations with the Board of Statutory Auditors and with the Independent Auditors during the audits and controls carried out by such Bodies, in compliance with the law.

Pursuant to Legislative Decree No. 231/2001, the process in question might offer opportunities for commission of the offence of "obstruction of controls", pursuant to Article 2625 of the Civil Code and of the offences referred to in Article 27 of Legislative Decree No. 39/2010 (with regard to the offence of false reporting or communications by the persons responsible for auditing, committed in conspiracy with bodies of the audited company) and in Article 29 of the same Decree (concerning the offence preventing or hindering the performance of statutory auditing activities), which are taken into account for the purposes of this protocol, notwithstanding the principle affirmed by the Court of Cassation mentioned, in paragraph 7.3.1 above.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the management of the relations in question.

Process description

In the context of the auditing activities proper to the Board of Statutory Auditors and the Independent Auditors, the management of relations between the Company's and/or outsourcer's structures and these entities is divided into the following activities:

- submission of the required periodic reports;
- submission of corporate information and data and provision of documentation, based on specific requests.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The control system for monitoring the process must be based on the following elements:

- Authorisation levels defined within each operating step of the process. In particular, relations with the Board of Statutory Auditors and the Independent Auditors shall be managed by the Head of the reference structure or by the persons specifically appointed by him.

- Regular and ongoing participation of the Board of Statutory Auditors in Board of Directors meetings, to ensure that the Board of Statutory Auditors is effectively informed of the Company's operational choices.
- Timely and complete processing, by the competent structures (of the Company or of the outsourcers, for the areas of their respective competence, by virtue of the service agreements entered into), of requests for specific documentation made by the Board of Statutory Auditors in the performance of its supervisory and control activities.
- Timely and complete processing, by the competent Structures (of the Company or of the outsourcers, for the areas of their respective competences, by virtue of the service agreement entered into), of requests for specific documents made by the Independent Auditors in performance of its audit, monitoring and administrative-accounting process assessment activities are promptly and fully met by the competent structures: each Structure shall collect and organise the information requested and deliver it, in accordance with the contractual obligations set out in the audit engagement contract. Records shall be maintained of all the documents provided in response to specific information requests formally made by the auditors.
- Timely and complete provision to the Audit Firm, by the structures concerned (of the Company or of the outsourcers, for the areas of their respective competence, by virtue of the service contract entered into), of the documentation they possess relating to the control activities and operational processes implemented, to enable the auditors to carry out their verifications.
- Process traceability including both the electronic and the paper trail:
  - all the monitoring and control activities carried out by the Board of Statutory Auditors shall be systematically recorded and kept on file;
  - storage of the letters, signed by the person with the necessary powers, to support the preparation of the Certification Report by the Independent Auditors;
  - in order to allow reconstruction of responsibilities and of the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it has produced relating to performance of the requirements relating to management of relations with the Board of Statutory Auditors and the Independent Auditors.

Rules of conduct

The Structures and Bodies of the Company (and, within their respective spheres of competence, the outsourcers, by virtue of the service agreements entered into), howsoever involved in the management of relations with the Board of Statutory Auditors and the Independent Auditors, have an obligation to act with the highest diligence, professionalism,

transparency, collaboration and availability and to fully respect the institutional role of said governance bodies, promptly and accurately meeting all provisions and performing any requirements set out in this protocol, in compliance with the applicable provisions of law and with any relevant provisions of the Group's Code of Ethics and Internal Code of Conduct.

Specifically:

- periodic communications to the Board of Statutory Auditors and the Independent Auditors must be punctually forwarded, and requests/enquiries received from them must be promptly acknowledged;
- all persons involved, including members of the Company's Board of Directors, who, for any reason whatsoever, are involved in a request for production of documents or information by the Board of Statutory Auditors or one of its members, as well as by the Independent Auditors, shall behave in a manner marked by utmost fairness and transparency and shall not hinder in any way the control and/or auditing activities;
- all data and documents shall be made available in a precise manner and using clear, objective and exhaustive language, so as to provide accurate, complete, faithful and truthful information;
- each Structure involved in the process is responsible for filing and storing all the documents formally produced and/or delivered to the members of the Board of Statutory Auditors, and to the Auditors, within the scope of their activity, including all documents submitted in electronic format.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- delay without good reason or omit the presentation of documents/communication of requested data;
- present incomplete documents and data and/or communicate false or altered data;
- adopt deceitful conduct which might lead the Board of Statutory Auditors and the Independent Auditors into error in the technical-economic assessment of the documents submitted;
- promise or give sums of money or other benefits to members of the Board of Statutory Auditors or Independent Auditors, with the purpose of promoting or furthering the Company's interests.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.3.2.2 Management of periodic reporting

This protocol applies to all the Company Structures involved in the preparation of the documents that contain communications to shareholders and/or to the market concerning the Company's profit and loss, balance sheet and financial situation, as well as communications to the subscribers of the Funds managed by the Asset Management Company relating to the performance of the Funds themselves.

Pursuant to Legislative Decree No. 231/2001, the process to prepare the documents in question could pose a risk of committing the offence of "false corporate reporting", as regulated in Articles 2621 and 2622 of the Civil Code, as well as tax crimes, indicated in paragraph 7.11 (Sensitive area concerning tax crimes).

Furthermore, the company rules and the controls of completeness and truthfulness envisaged in this protocol are also arranged with a view to providing more extensive preventive action against offences that could arise from incorrect management of financial resources, such as "*bribery*" in its various forms, "*illegal inducement*" "*private-to-private corruption*" and "*instigating private-to-private corruption*" as well as the offences of "*money laundering*" and "*self-laundering*".

Since the Company is not listed, it has no obligations with regard to the identification of the figure of the "Financial Reporting Officer". It is consolidated on an equity accounting basis and the related process, where applicable, is governed by specific guidelines, including Intesa Sanpaolo's "*Administrative and Financial Governance Guidelines*", whose principles the Company incorporates.

Besides the above Guidelines, specific governance documents and rules, updated from time to time and insofar as they are applicable, are used for the governance and process of preparing documents containing communications to the shareholders and/or to the market concerning the Company's financial position and performance and cash flows, including:

- the "Guidelines for the governance of financial disclosure to the market (Financial Statements and Pillar III);
- "Guidelines for evaluating financial statement items";
- "Group accounting rules";
- regulations on Fair Value;
- "Rules on preparing disclosure to the public Pillar III".

The Company has also adopted specific internal procedures defining the reference principles, roles and responsibilities assigned to the Company structures concerning the preparation of the documents covered by this protocol. These procedures are to be considered an integral part of this protocol.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

In the context of sensitive processes for the purposes of financial reporting, of particular importance are the activities strictly functional to the production of the annual and interim financial statements and the activity of measuring the equity investments held by the Funds managed by the Company. Such activities fall under the following corporate processes:

- Management of the accounts and of supervisory communications;
- Management of company Financial Statements;
- Measurement of the Funds' holdings for reporting purposes;
- Preparation and editing of periodic reports for Fund subscribers.

A further sensitive activity for financial reporting purposes concerns the process of identifying and managing relationships with related parties.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The documents containing communications to the shareholders and/or to the market concerning the Company’s profit and loss, balance sheet and financial situation or communications to subscribers on the performance of the Funds managed by the Company must be prepared in accordance with the specific corporate procedures, practices and systems in force which:

- identify in a clear and exhaustive manner the functions concerned and the data and information they must provide;
- identify criteria for recognising corporate events in the accounts, including the recognition of individual items;
- define the deadlines, the matters to be communicated and disclosed, organisation of the related flows of information and any request for the issue of specific declarations;
- provide for the transmission of data and information to the Structure responsible for collecting them through a system that ensures the traceability of the individual transactions and identification of the persons that enter the data into the system;
- provide criteria and procedures for the processing of the Company's data necessary for the preparation of the Group's consolidated financial statements and their transmission to the Parent Company.

The control system for monitoring the process described above must be based on the following elements:

- Specifically defined roles and responsibilities:
  - each single Structure (of the Company or of the outsourcers, for the areas of their respective competences, by virtue of the service agreement entered into) is responsible for the processes contributing to the production of the accounting items and/or measurement activities assigned to it and of any comments in the financial statements or in the documentation towards the subscribers of the Funds under its competence;
  - different user profiles are defined for accessing IT procedures, matching specific authorisation levels based on assigned functions;
- Segregation of functions:
  - the process of preparing documents containing communications to shareholders and/or the market relating to the Company's profit and loss, balance sheet and financial situation, or communications to subscribers on the performance of the Funds managed by the Company, involves several Structures (of the Company and of outsourcers under the service agreements entered into), operating in the various stages of the process for their respective areas of competence and on the basis of the Company's internal procedures.
- Control activities:
  - the activities of preparing documents relating to the Company's profit and loss, balance sheet and financial situation, which contain communications to shareholders and/or, through the Parent Company, communications to the market, as well as communications to the subscribers of the Funds, shall be carefully and thoroughly checked for completeness and accuracy, using both automated and manual systems. The main controls performed by the individual Structures are as follows:
    - periodic checks of the balances of the accounting items in general, in order to ensure the reconciliation with the respective management data;
    - verification, at predetermined intervals, of all balances of contract work, accruals/deferrals and similar accounts, to ensure their actual value;
    - existence of maker and checker controls ensuring that the person executing the transaction is different from the person who authorised it after checking its appropriateness;

- any changes are analysed by comparing the accounting data for the current period with that recorded in the previous periods and with the expected budget balances;
- a control on the merit is carried out when opening new accounts and updating the account plan;
- cross-examination between different Structures of the Company or of the outsourcer in respect of particularly significant valuation activities, as well as the assignment to a specific function, endowed with adequate expertise and independent from the fund management structures, of the valuation activity of the companies in which the Fund has an interest;
- harmonisation of the final version of the financial statements with the accounting data.

- Process traceability including both the electronic and the paper trail:
  - the decision-making process for preparing the documents containing communications to the shareholders and/or, through the Parent Company, to the market concerning the Company's profit and loss, balance sheet and financial situation is guaranteed by the complete traceability of each accounting operation, both via the IT system and on paper support;
  - all adjustment entries made by the Structure in charge of managing the Financial Statements or preparing reports for the subscribers of the Funds managed by the Company are supported by adequate documentation from which it is possible to infer the criteria adopted and (analytically) the development of the relevant calculations;
  - all the documentation concerning the periodic controls carried out shall be kept on file by the Structure involved in respect of the accounting items under its competence;
  - all supporting documentation for the preparation of the financial statements, other periodic reports and due disclosures is filed at the competent Structures (of the Company or of the outsourcers).

Rules of conduct

The Structures of the Company and of the outsourcers by virtue of the service agreements entered into, howsoever involved in bookkeeping activities and the subsequent preparation/filing of corporate communications on the Company's profit and loss and asset situation (financial statements, management report, periodic reports, etc.) and performance of the managed Funds (Annual Report and Half-Yearly Report) are required to comply with the procedures set forth in this document, with the relevant provisions of law, as well as

with the specific internal procedures based on the principles of transparency, accuracy and completeness of accounting information in order to produce fair and timely views of the profit and loss, asset and financial situation, also in accordance and for the purpose of Articles 2621 and 2622 of the Civil Code. In particular, all those involved in the process are required to:

- represent operations correctly, completely and promptly in the company accounts and data, in order to guarantee a true and fair view of the financial position, performance and cash flows of the Company and the Funds managed;
- adopt at all times a correct, transparent and cooperative approach, in compliance with the rules of law and with internal corporate procedures, in all the activities for the preparation of the financial statements and other corporate disclosure, in order to provide shareholders and third parties with a true and fair view of the financial position, performance and cash flows of the Company and the performance of the Funds managed.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- recognise or transmit for processing and recognition in financial statements, reports and prospectuses or in other corporate communications, false, incomplete or howsoever inaccurate data on the profit and loss, balance sheet and financial situation of the Company and the performance of the Funds managed;
- omit data and information imposed by the law on the profit and loss, balance sheet and financial situation of the Company and the Funds managed.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.3.2.3 Purchase, management and disposal of investments and other assets

This protocol applies to the structures of the Company involved in the purchase, management and disposal of investments – direct or indirect, qualified or unqualified – in the share capital of other companies, and other forms of investment/disinvestment similar to the undertaking/disposal of an equity investment (such as, for example, the subscription of convertible bonds or equity instruments) and other assets (for example, non-performing loans, business units, assets and legal relationships identified in blocks).

Pursuant to Legislative Decree No. 231/2001, the related process could present opportunities for the commission of "*private-to-private corruption*" and *"instigating private-to-private corruption*", "*Failure to disclose conflict of interest*" and "*"False or omitted statements for the issuance of the preliminary certificate"*. The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The process can be broken down as follows:

- examination of the feasibility of the transaction and/or identification of investment and/or funding opportunities;
- management of pre-contractual relationships and performance of activities preliminary to the signing of the contract (regulatory compliance verification, due diligence, etc.);
- finalisation of the contract;
- management of the obligations related to the purchases, management and disposal of investments (including the assignment of officers to the investee and cross-border merger transactions) and other assets.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The system of controls for monitoring the process described is based on the following factors:

- Expressly defined authorisation levels. Specifically:
  - the persons exercising authorising and/or negotiating powers at each stage of the process are identified and authorised in accordance with the provisions of the Articles of Association or the powers specifically delegated to them, as set out in the

Company's Organisational Manual and Functional Chart, or specifically assigned by means of proxy (to be kept by the Structure concerned) by the persons empowered;

- instruments and documents binding to the Company must be signed by persons with the necessary powers to do so;
- the delegated powers system establishes the right of independent management in relation to investments; internal regulations illustrate the aforementioned authorisation mechanisms, providing an indication of the corporate officers holding the necessary powers.

- Segregation of duties among persons involved in the process in order to guarantee maker and checker mechanisms between the phases of the process.
- Control activities:
  - verification of the preliminary investigation carried out in accordance with the provisions of the investment policies of the managed funds and of the internal rules and regulations, including through the possible performance of specific due diligence activities (e.g. economic/financial, accounting, legal, tax, etc.) on the company being invested in (so-called "target company") and the counterparty particularly with regard to the provisions of the Anti-Corruption Guidelines;
  - verification that the resolution contains the transaction pricing criteria in accordance with market practices;
  - verification of compliance with legal and regulatory obligations (e.g. regarding anti-trust, anti-money laundering, etc.);
  - verification of the keeping and updating of records of existing investments;
  - verification of the periodic assessment process for existing investments as part of the preparation of periodic reports.
- Process traceability including both the electronic and the paper trail:
  - each significant phase of the activity regulated by this protocol must be recorded in a specific written document;
  - every agreement/convention/contract/other formality instrumental to the purchase, management and disposal of investments and other assets is formalised in a document duly signed by persons with suitable powers to do so on the basis of the existing delegated powers system;
  - in order to allow reconstruction of the responsibilities and motivations underlying the preliminary assessment conducted for making the investment and the decisions made during its management and disposal of investments and other assets, each Structure involved in the process is responsible for archiving and storing the documentation it produces, also digitally or electronically, in relation to this protocol.

- Bonus or incentive systems: Group bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of conduct

The Structures of the Company and of the outsourcers by virtue of the service agreements entered into, howsoever involved in the process of acquisition, management and disposal of equity investments and other assets, are required to comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Code of Ethics, the Group Internal Code of Conduct and the Anti-Corruption Guidelines of the Group. Specifically:

- persons exercising authorisation and/or negotiating powers at the pre-contractual, contractual and management phases of investment relationships must be identified and authorised on the basis of their specific role assigned by the Organisational Manual or Functional Chart or by the Head of the reference Structure by means of an internal delegation, kept on file by the same Structure;
- documentation relating to contracts for the purchase, management and disposal of investments and other assets must comply with current general and special regulations for the reference sector, also by seeking advice from external professionals;
- the persons involved in the process may not comply with any request for money or other benefits which they may receive or become aware of, formulated by senior officers, or their staff, belonging to companies which are counterparties to or in relation with the Company, aimed at the performance or omission by the latter of an act contrary to the obligations inherent to their office or to the obligations of loyalty, and must immediately report it to their Manager; the latter in turn is obliged to forward the report received to the Structure in charge of Internal Auditing and to the Corporate Anti-Corruption Officer for the relevant evaluations and possible compliance with the Surveillance Body in accordance with Chapter 4.1;
- if the involvement of third parties is envisaged in the signing and/or management of contracts relating to the purchase, management or disposal of investments and other assets, the agreements with such parties must contain a special declaration of awareness of the regulations contained in Legislative Decree No. 231/2001 and the provisions of the laws against corruption and a commitment to comply with such regulations;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for

assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by current or future activities;

- the persons appointed by the Company as members of the administrative body of an investee company are required to notify the latter – in the form and within the terms provided for by Article 2391 of the Civil Code – the interest they have, either on behalf of the Company or on their own behalf or on behalf of third parties, in a certain transaction of the company in question, refraining from carrying out the transaction if they are a Chief Executive Officer.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- communicate false or altered data;
- promise or pay/offer undue sums of money, gifts of services free of charge (outside the accepted practices of courtesy gifts of little value) and grant advantages or other benefits of any kind – directly or indirectly, for oneself or for others – to directors, general managers, managers in charge of preparing the company's financial statements, statutory auditors or liquidators of companies, or persons under their management or supervision, in order to obtain from such persons the performance or failure to perform an act contrary to their official duties or obligations of loyalty to further or favour the interests of the Company. Advantages that could be granted include, by way of example, the promise of employment for relatives and relatives-in-law, sponsorship or charity for the benefit of connected persons and, more generally, all those banking and financial transactions that result in the generation of a loss for the Company and the creation of a profit for the aforementioned persons;
- award appointments to external consultants without following substantiated and objective criteria addressing professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of consultants shall refer to the criteria of clarity and availability of documentary evidence laid down in the Group's Code of Ethics, Internal Code of Conduct and Anti-Corruption Guidelines.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.4 Sensitive area concerning receipt of stolen goods, money laundering and use of unlawfully obtained money, goods or benefits, as well as self-laundering

7.4.1 Type of offence

Legislative Decree No. 231 of 21.11.2007, (hereinafter, the anti-Money Laundering Decree) and Legislative Decree No. 109 of 22.6.2007, which transposed Community law have strengthened the legislation on the prevention of the use of the financial system for the purpose of money laundering and on the fight against the financing of terrorism.

Article 25-octies of Legislative Decree No. 231/2001, introduced by the anti-money laundering Decree, extended the Entity's liability to cover the receipt of stolen goods, money laundering and unlawful use, even in the cases in which these acts are not committed for terrorist purposes or for subversion of the democratic order – covered by Chapter 7.5 – or where they do not have the transnational characteristics[42]. Finally Article 25-octies was amended adding the new offence of self-laundering[43].

The reinforcing of the legislation on the administrative liability of Entities aims to prevent and combat more effectively the phenomenon of the introduction into lawful economic circuits of money, goods or other assets which are the proceeds of crime, as this hinders the activities of the justice system in detecting offences and prosecuting offenders, and in general damages the economic order, market integrity and free competition, by reason of the unfair competitive advantage enjoyed by those operators who have at their disposal financial resources of unlawful origin.

On a different plane, albeit still for the purpose of combating money laundering and of the financing of terrorism, but from another perspective, the anti-Money Laundering Decree establishes specific requirements for banks and financial intermediaries in general (appropriate checks on customers; recording and storage of transaction documents; reporting of any suspicious transactions; notification of any infringements of the prohibitions concerning cash and bearer securities; reporting by the Entity's control and Audit Bodies of any infringements identified). Infringement of said obligations of itself but does not give rise to the Entity's administrative liability under Legislative Decree No. 231/2001, since such offences are not included in the list of the so-called predicate offences (i.e. the offences giving rise to the Entity's administrative liability) but is punished pursuant to the anti-money laundering Decree, in accordance with a policy of preventive safeguards irrespective of whether money laundering offences are materially committed, to ensure compliance in all cases with the fundamental principles of in-depth knowledge of customers and the

[42] See Chapter 7.5.1 for details. It should be noted that pursuant to paragraphs 5 and 6 of Article 10 of Law No. 146/2006, repealed by the anti-money laundering Decree, money laundering and unlawful use of money were considered to be offences giving rise to the liability of Entities only if the transnational characteristics laid down in Article 3 of the same Law were met.

[43] The new offence of self-laundering was introduced in the Criminal Code and added to the presumed crimes of Legislative Decree No. 231/2001 by Law No. 186/2014, that came into force on 1.1.2015.

traceability of transactions, to avoid any danger that financial intermediaries might be unwittingly involved in illegal activities.

It should be noted that if the financial operator fails to perform his obligations being fully aware of the illegal origin of the goods subject of the transactions, he could be indicted for such offences, and consequently the Company might incur administrative liability under Legislative Decree No. 231/2001.

The constituent elements of the offences in question are briefly illustrated below.

Receipt of stolen goods (Article 648 of the Criminal Code)

This offence occurs when any person, for the purpose of obtaining a profit for himself or for others, purchases, receives or conceals money or goods deriving from any offence whatsoever, in whose commission he did not participate, or in any case concurs in their purchase, receipt or concealment. In order for this offence to occur, the perpetrator must act with malice, i.e. knowingly and with the intent of obtaining a profit for himself or others, by purchasing, receiving or concealing stolen goods.

Moreover, the offender must also be aware of the criminal origin of the money or the goods; the presence of this psychological condition can be signalled by serious and concurring circumstances: for instance the quality and the characteristics of the goods, the unusual economic and contractual terms and conditions of the transaction, the personal condition or employment of the holder of the goods – leading to the conclusion that the author of the act must have been certain of the illegal origin of the money or the goods.

Money laundering (Article 648-bis of the Criminal Code)

This offence occurs where a person, who did not aid and abet commission of the underlying crime, substitutes or transfers money, goods or other assets deriving from a non-negligent offence or carries out other transactions in respect of such money, goods or assets, so as to obstruct identification of their criminal origin.

The purpose of this provision is to punish those who – being aware of the criminal origin of the money, goods or other assets – perform the above-mentioned transactions, in such a way as to materially hinder discovery of the illegal origin of the goods in question.

For the offence to occur, the culprit needs not have acted for the purpose of obtaining some gain or of helping the perpetrators of the underlying crime to secure the proceeds of their crime.

Money laundering consists of dynamic actions aimed at putting the goods into circulation, whereas their mere receipt or concealment could give rise to the offence of receipt of stolen goods. Similarly to the offence of receipt of stolen goods, the offender's awareness of the

illegal origin of the goods can be determined on the basis of any serious and univocal objective circumstance.

Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)

This offence occurs when any person uses money, goods or other proceeds of crime in economic or financial activities, with the exclusion of cases in which the perpetrator was also complicit with the underlying crime and with the exception of the offences set out in Article 648 (Receipt of stolen goods) and Article 648-*bis* (Money laundering) of the Criminal Code.

Compared with the offence of money laundering, while the same subjective element of awareness of illegal origin of the goods applies, Article 648-ter restricts the scope of this offence to cases in which such proceeds of crime are employed in economic or financial activities. However, given the comprehensiveness of the definition of the money laundering offence, it is hard to imagine any use of goods of illegal origin which would not fall under the scope of Article 648-bis of the Criminal Code.

Self-laundering (Article 648-ter.1 of the Criminal Code)

The offence of self-laundering is committed by any person who, having committed or having conspired to commit any non-negligent offence from which money, goods or other benefits originate, uses, replaces or transfers such proceeds in economic, financial, entrepreneurial or speculative activities, in such a way as to concretely hinder the identification of their criminal origin.

This excludes liability to punishment of conduct consistent with the allocation of the illegal proceeds for the mere personal use or enjoyment. The sentence may be increased if the fact is committed when conducting professional, banking, or financial activity and may be reduced in the event of voluntary disclosure by the guilty party.

Remarks applying to the offences

<u>Material subject</u>

The material subject of these offences can consist of any asset having appreciable economic value and which may be exchanged, such as money, credit securities, means of payment, credit entitlements, precious metals/gems, tangible and intangible assets in general. These goods or assets must originate from the offence, i.e. they must be the product (the result or benefit obtained by the offender by committing the crime), the proceeds (monetary gain or economic benefit obtained from the offence) or the price (amount paid to induce, instigate, or lead someone to commit the offence). In addition to the

offences typically aimed at the creation of illegal capital (for example, extortion in office, bribery, embezzlement, fraud, bankruptcy crime, arms or drug trafficking, usury, fraud against EU funds, etc.) and tax offences could also give generate to proceeds which are then laundered or of self-laundering, not only for fraud (for ex., the use of invoices for non-existent transactions that result in a fictitious credit; VAT to be deducted) but also in the case in which the economic utility consequential to a crime consists in a mere tax saving due to the non-disbursement of money originating from legal activities, (for example, failing to report or misreporting the income for amounts above the threshold of criminal relevance).

Conduct and subjective element

A third party not involved in the original offence that generates illegal proceeds and who receives them from the original offender (or from others, however knowing of the illegal origin) to perform conduct thereupon provided for by the said crimes shall be answerable to the crimes of receipt, laundering or illegal reuse of stolen goods.

A party who provided any type of moral or material causal contribution to the commission of the original offence for example determining or strengthening the criminal intent of the original offender with the promise, even before the commission of offence, his help in the recycling/using the proceeds could instead be answerable to conspiracy in the crime that generated the illegal proceeds and, consequentially, also in the subsequent crime of self-laundering, should he carry out the conduct.

The crime of self-laundering, unlike as prescribed for crimes of money laundering and of unlawful use, requires that the conduct be characterized by methods suitable for the actual masking of the true criminal origin of the goods; the interpretation of the most innovative aspects of the law – that is to say requirement of the actual hindrance and the condition of non-liability to punishment of the self-launderer for personnel use (which would again seem to be excluded if the original offence and the reuse take place in the performance of a business activity) – shall necessarily refer to the jurisprudential applications of the crime.

As to the subjective element, as already stated, the offences in question must be marked by awareness of the fact that the goods in question are the proceeds of crime. According to a particularly strict interpretation, the offence may also occur if the person dealt with the goods while harbouring suspicions as to their illegal origin, accepting such risk (“dolus eventualis" or indirect intention). With reference to banking or financial operations , it should be noted that the presence of anomaly indicators or anomalous conducts as set out in the measures and in the patterns issued by the competent Authorities (as concerns financial intermediaries, by the Bank of Italy and by the UIF (Unità di Informazione Finanziaria) - Finance Intelligence Unit) in specific concrete situations might, if the particularly strict

interpretation mentioned above is adopted, be considered as a serious and univocal objective circumstance which should give rise to doubts as to the illegal origin of the goods.

Correlations with the original offence related to the illicit gains

The crimes of this Sensitive area subsists the cases in which the relative conduct is subsequent to the perfecting of the crime that was the origin of the illicit gains, even if performed after its extinction (for example due to the statute of limitation or death of the original offender), or also if the author of the crime is not chargeable or liable to punishment, or if the condition for prosecution do not exist (for example, no lawsuit has been filed, or upon request by the Minister of Justice, necessary to pursue common crimes common committed in foreign countries overseas, pursuant to articles 9 and 10 of the Criminal Code)[44].

7.4.2 Sensitive company activities

The risk of money-laundering offences, understood in the broadest sense (including, therefore, self-laundering), occurring in the Company's operating context, appears indeed more marked, as a risk typical of the banking and financial circuit, essentially with reference to relations with third parties or with the subscribers of the managed Funds, who could channel the sums deriving from illegal activities into the Funds themselves[45].

Prevention activity is based on in-depth knowledge of customers and counterparties and on compliance with the legal requirements relating to the fight against money laundering and the financing of terrorism.

The central importance of strict compliance with the provisions dictated by the anti-money laundering Decree for the purpose of prevention the presumed crimes in question also follows from the subsequent considerations. It should first of all be stated that the Decree – for the purpose of identifying the type of conduct at risk for money laundering, and subject to the reporting requirements of suspicious transactions – defines, under Article 1 “transaction” as the transmission or the movement of means of payment” and contains a list, under Article 2, of conduct, characterized as money laundering, of very broad extension, so as to include conduct which, for criminal purposes, could include the commission of the crime of self-laundering, or the commission of other the predicated offences in question and that, if carried out by employees or by top-managers, could entail administrative liability of the Entity itself. Finally, the above-mentioned list also includes atypical conduct relating to other offences, such as aiding and abetting an offender (Article

[44] With regard to the irrelevance of extinction of the offence that constitutes the grounds for another offence see Article 170, paragraph 1 of the Criminal Code; For the irrelevancy of the lack of a condition of liability to punishment or prosecution, see Article 648, paragraph 3, of the Criminal Code, also cited by Articles. 648-bis, 648-ter and 648-ter.1 of the Criminal Code.

[45] On the other hand, the activity of acquisition of participations by the Managed Funds is not relevant for the purposes of anti-money laundering regulations as it is carried out at the initiative of the Company (ref. Provision laying down implementing provisions on customer due diligence to combat money laundering and terrorist financing of 30 July 2019).

378 of the Criminal Code) which, where it is of a transnational nature (on this point see Chapter 7.5) can also constitute a predicate offence for the administrative liability of Entities.

The risk takes on different connotations and appears less relevant when considering the Asset Management Company as a "company", with reference to those areas in which the Asset Management Company, even apart from the performance of its typical activities, carries out instrumental transactions, acquires shareholdings or moves its assets, and fulfils accounting and tax obligations. In these areas in fact there is a well-developed articulation of control system and procedures already established by the legislation in the sector in order to ensure the observance of the principles of transparency, correctness, objectivity safeguards and the traceability of management.

We reproduce below the protocol laying down the control principles and rules of conduct applicable to the management of the risks relating to the financial fight against terrorism and money laundering. The protocols regulating other sensitive activities – such as Management of disputes and of out-of-court settlements (Chapter 7.2.2.4), Management of the procedures for the procurement of goods and services and for the appointment of professional consultants (Chapter 7.2.2.6) and Management of gifts, entertainment expenses, donations to charities and sponsorships (paragraph 7.2.2.7) – also include certain control and conduct principles based on the same criterion of thorough assessment of suppliers, consultants and contractual counterparties in general, and which can also help prevent the offences addressed in this section.

More generally, all the protocols of this Model, where meant to prevent the committing of offences that can generate illicit gains, must also be understood to meant to prevent money laundering offences in a broad sense. We cite especially the protocols relative to the Sensitive areas concerning corporate offences – in particular, the protocol on the Management of periodic reporting (Chapter 7.3.2.2) – the offences and regulatory offences ascribable to market abuses and computer crime.

All the foregoing protocols are supplemented by detailed corporate regulations governing such activities and also apply to the monitoring of any activities performed by outsourcers or other Group companies on the basis of special service agreements.

7.4.2.1 Financial combat against terrorism and money laundering

The purpose of this protocol is to define the roles, operational responsibilities and control and conduct principles relating to the financial fight against terrorism and money laundering.

Taking into account the specific operations of the Company, the offences in question could be committed in the context of subscription transactions of the units of the Funds managed by the Company if the counterparty were to set itself the objective of "cleaning up" assets of unlawful origin, wrongfully acquired, through transactions of this kind.

This protocol applies to all the structures of the Company and of the outsourcers involved in the subscription activities of the Funds' units and in the consequent flows of means of payment connected to the call of commitments and redemptions, even partial, of units of the Funds.

The protocol refers to applicable company provisions, and in particular the Parent Company's Guidelines for combating money laundering and terrorist financing and for managing embargoes and the Company's internal regulations applicable from time to time.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

For the purposes of combating the financing of terrorism and money laundering, the following operational areas are pertinent:

- identifying and knowing the customers and the persons on behalf of whom they operate, assessing their risk profile, i.e. the likelihood of exposure to phenomena of money laundering activities financing terrorism by means of a specific profiling procedure. Risk assessment is based on an in-depth knowledge of the persons concerned and takes into account, in particular, objective aspects (activities carried out by customers, transactions carried out by them and the instruments used[46]) and subjective aspects (persons subject to enhanced due diligence obligations; persons located in countries/centres characterised by privileged tax or anti-money laundering regimes such as those identified by the FATF as "non-cooperative", etc.). Particular attention must be paid to detecting any possible involvement in transactions or in relationships with persons (both natural and legal persons) that are included in public lists published both at national and international level (UN, EU, OFAC and MEF, ABI-UIF lists, hereinafter all referred to as "Black Lists");

[46] For instance, the interposition of third parties, the use of corporate, associative or trust instruments likely to limit transparency with regard to the ownership and management structure.

- opening of new ongoing relationships and updating/review of the information on existing customers, to ensure compliance with the principle of the “know your customer” rule;
- monitoring of operations and ongoing assessment of the risk of money laundering or financing of terrorism, based on specific timelines and procedures defined according to risk profile levels;
- assessment of the transactions ordered by customers with persons/Countries/goods which are subject to financial restrictions (freezing of assets and resources, prohibition of financial transactions, restrictions on export or investment) and/or commercial restrictions (general or specific trade sanctions, bans on imports and exports, such as a weapons embargo);
- discharge of regulatory obligations on the retention and availability of documents, data and information to combat money laundering and terrorist financing;
- external reporting to the Supervisory Authorities and internal reporting for the purpose of preparing the external reports.

The operating procedures for the management of the above-mentioned processes are governed by the internal rules, which are developed and updated by the competent Structures, form an integral and substantive part of this protocol, and have been drawn up in accordance with the Parent Company’s "Guidelines for Combating Money Laundering and Terrorist Financing and Managing Embargoes".

Control principles

The control system for monitoring the processes described above is based on the following elements:

- Clearly defined responsibilities:
  - the internal set of rules identifies the individuals and Structures responsible for initiating//managing/controlling the processes described above;
- Segregation of duties:
  - in the situations identified by legal provisions and internal regulations imposing enhanced customer due diligence obligations, the opening of new relationships, the execution of transactions and the maintenance of pre-existing relationships are subject to the issue of an authorisation by the Chief Executive Officer of the Company;
  - in order to detect potentially suspicious transactions, there is a segregation whereby:
    - the person in charge who, during the investigation phase or in the course of carrying out the operation, identifies the prerequisites for the identification of a

suspicious transaction, shall report it to their Manager for further investigation and possible reporting;

- the Manager, on the basis of the information in their possession, shall, if the transaction is suspicious, refer the matter to the Manager responsible for reporting suspicious transactions;
- such Manager responsible for reporting suspicious transactions shall analyse the report so received and shall carry out the necessary investigations on the suspicious transaction, deciding whether or not the reports should be forwarded to the competent Authority.

- Control activities: the control system for monitoring the process described above is based on the following elements:
  - in the context of a precise profiling of customers, verified according to a risk-based approach, when the relationship is established or when the transaction is carried out, by the Manager of the operational structure concerned:
    - the correctness and completeness of the data acquired for the identification of the counterparty and in relation to the economic activity carried out, in accordance with the processes defined by the procedures in force; this information must be updated, from time to time, in relation to the economic reasons underlying the transactions requested or carried out;
    - the presence of anomalies on the counterparty in order to identify involvement in unlawful activities, the possible presence of the name in the updated versions of the "black lists", as well as the performance of transactions with persons/countries/goods subject to financial restrictions (freezing of assets and resources, prohibition of financial transactions, investment restrictions) and/or trade restrictions (general or specific trade sanctions, import and export bans such as weapons embargo);
  - medium/long-term monitoring by the competent operational Structures which ensures cross-checking between the customer's subjective profile, the type of transaction, the frequency and method of execution, the reference geographical area (with particular regard to transactions from/to Countries at risk) and the degree of risk attributed to the product involved in the transaction, the funds used, the time horizon of the investment, the conduct of the customer at the time of execution of the transaction (if the transaction is carried out in the customer's presence), in accordance with the times and procedures established by the specific internal procedure;

- monitoring and supervision by the Manager of the Operational Structure with regard to the acquisition and storage of the information necessary for the identification and profiling of customers, as well as the constant updating thereof;
- recording of all ongoing relationships and transactions with the prerequisites required by anti-money laundering legislation in the Single Computerised Data File with correct and complete data. An orderly archive makes it possible, among other things, to deal promptly with requests for information from the competent authorities and to reconstruct customer transactions.

- Process traceability including both the electronic and the paper trail:
  - in order to allow reconstruction of responsibilities and of the reasons for the choices made, the Structure from time to time concerned shall be responsible for filing and storing, also in telematic or electronic format, all the documentation it produces relating to performance of the requirements associated with the process described; in particular:
  - confidential and orderly storage, by the Structure in charge of managing counterparty relationships, of all documentation relating to the identification and profiling of customers, as well as the controls carried out on counterparties;
  - full records shall be kept of the decisions and justifications made regarding any change in the customer's profile or the establishment/maintenance of relationships with high-risk counterparties;
  - keeping in strict confidence the decisions and reasons given on whether or not to forward a suspicious transaction report to the competent authorities and the relevant supporting documentation.
- Information shall be kept confidential, in particular that concerning identification of real account holders, customer profiling and suspicious transaction reporting processes.
- Training: activities specifically focused on continuous training of employees and collaborators in identifying the risk profiles associated with the legislation on anti-money laundering and combating terrorism financing shall be provided on a regular basis.

Rules of conduct

The Structures of the Company and of the outsourcers by virtue of the service agreements entered into, howsoever involved in the financial fight against terrorism and money laundering, are required to comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Groups Code of Ethics and Internal Code of Conduct.

In particular the competent Structures have an obligation to:

- ensure the development and implementation of the applications used in the financial fight against terrorism and money laundering and in any case in all the activities based on “appropriate due diligence of customers”;
- ensure that customers operate in compliance with the restrictions and the authorizations provided for by the embargo measures or by the rules governing the export of particular types of goods and/or materials (e.g. dual-use goods, hazardous chemical substances);
- establish detailed rules of conduct in the internal regulations/operating rules, supplementing and expanding on the external legislation and the principles laid down in this protocol;
- where the counterparty or transaction assessment involves more than one operational Structure or Intesa Sanpaolo Group company, the Structures or companies concerned shall co-operate with each other and, where allowed by current legislation, shall exchange information for the purpose of acquiring comprehensive and appropriate knowledge of the counterparty and of the typical transactions he engages in;
- ongoing and systematic training and updating shall be delivered to staff on anti-money laundering legislation and embargoes and on the aims pursued by such provisions;
- the reference legislation and all updates thereof shall be disseminated to all employees, regardless of their actual duties;
- verify and ensure the dissemination within the Company's structures of restrictive measures – containing operational limitations in specific sectors – and updated “black lists”.

Furthermore, all employees and collaborators acting in compliance with company procedures must:

- at the time of activating ongoing contractual relationships or executing transactions exceeding the legal threshold, even if fractionated:
  - proceed to the identification of the counterparty, through the acquisition of a photocopy of a valid identification document and the tax code, after checking whether the name is on the updated versions of the “black lists”;
  - verify the identity of actual account holders, obtain information on the purpose and nature of the relationship or transaction and, where the customer is a company or an Entity, verify that the person requesting the transaction holds due authority to sign, and check the customer’s ownership and control structure;
  - carry out customer profiling and due diligence;
- regularly update all data concerning ongoing relationships to allow continuing assessment of the counterparty’s economic and financial profile;

- perform the customer verification and profiling process where, regardless of any applicable amount threshold or exemption, suspicions of money laundering or of the financing of terrorism are harboured, or doubts arise as to the truthfulness or adequacy of already acquired identification details;
- keep information concerning the anti-money laundering risk level assigned to the customer and the relevant score calculated by the procedure strictly confidential; such information may not be disclosed to customers under any circumstance;
- not to execute transactions involving persons/countries/goods subject to financial and/or commercial restrictions or for which there is any suspicion of a relationship with money laundering and terrorist financing;
- consider whether to initiate a reporting process where abnormal indicators are detected, even if such abnormalities were not signalled by IT procedures, or where it is impossible to comply with the appropriate verification requirement;
- actively participate in the processes of detecting and reporting suspicious transactions;
- comply with the internal procedures on the recording of relationships and transactions in the financial transaction database (AUI) and on the filing of documentation.

All persons in charge of the assessment and authorisation activities set forth by the anti-money laundering processes, must exert their discretion according to professionalism and reasonableness. In the event of personal or corporate conflicts of interest, even if potential, they must:

- immediately report to their manager about the conflict of interest detailing its nature, terms, origin and relevance;
- refrain from assessment/authorisation activities, delegating decisions to their manager or to the appropriate Structure as defined by the internal regulations. By way of example, conflict of interest may occur if personal interests interfere (or seem to interfere) with the Company's or the Group's, thus hindering the effective and impartial performance of one's activities, or if inappropriate personal benefits are pursued based on the position held within the Company or the Group.

Employees are furthermore forbidden to inform, even unintentionally, third parties (including their family members, close relations or their family's close relations) about the result of any assessment/authorization activity in any circumstance not provided by the law for reasons other than those pertaining to office activity.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- set up ongoing relationships, or maintain existing ones, and execute transactions when it is impossible to fulfil the obligation of appropriately checking the customer's details, for instance when the customer refuses to provide requested information;
- execute transactions which are suspected of being linked to money laundering or terrorism financing schemes;
- receive or conceal money or assets obtained through any criminal act, or carry out any activity which may facilitate the purchasing, receipt or concealment of such proceeds of crime;
- replace or transfer money, goods or other assets originating from offences, or execute any other transactions in respect of such assets which might obstruct identification of their criminal origin;
- take part in one of the acts listed in the above bullet points, conspire with others to commit them, attempt to commit them, aid and abet, instigate or advise anyone to commit them or assist in their execution;
- make available to customers who belong to or are howsoever close to criminal organisations any services, financial resources or other economic means which may be instrumental to the pursuit of illegal activities.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

The principles of control and conduct set out in this protocol are also to be understood as applicable, to the extent of their compatibility, in the event of cross-border mergers involving the Company.

7.5 Sensitive area concerning crimes with the purpose of terrorism or subversion of the democratic order, organised crime, transnational crimes and crimes against the person, as well as sports fraud and illegal betting or gaming

7.5.1 Type of offence

Through a series of legislative acts, the framework of the administrative liability of Entities has been expanded to include various categories of offences, with the common aims of combating types of crime which raise particular concern at international level, specifically crimes of political terrorism, organised crime, including international organised crime, and crimes which violate fundamental human rights.

The Company places particular attention and commitment in collaborating in the fight against terrorism and the prevention of criminal phenomena in the financial market, a commitment that the Company also assumes for the purposes of safeguarding sound and prudent management, transparency and correct behaviour and the proper functioning of the financial system as a whole. In theory, the Company could establish relations with counterparties belonging to or in any case close to organised crime by making available financial resources or economic assets that are instrumental to the pursuit of unlawful activities.

The types of crimes in question are summarised below.

Section I - Crimes for the purposes of terrorism or subversion of the democratic order

Under Article 25-*quater* of the Decree an entity shall be punishable, where there are appropriate grounds, in the event that the crimes for the purpose of terrorism or subversion of the democratic order provided for by the Criminal Code, the special laws and by the International Convention for the Suppression of the Financing of Terrorism signed in New York on 9/12/1999, are committed in the interest of or for the benefit of the entity.

This provision sets out no fixed or mandatory list of crimes, but refers to any criminal offence whose author specifically pursues aims of terrorism or subversion of the democratic order[47].

The main types of such offences which might apply are briefly described below.

[47] Article 270-sexies considers as having terrorist purposes those conducts which can cause considerable damage to a Country or international organization and are committed in order to intimidate the population or force public authorities or an international organization to perform or restrain from performing any deed or destabilize or destroy fundamental political, constitutional, economic and social structures, as well as the other conducts defined as terrorist or committed for the purpose of terrorism by conventions or other international law provisions which are binding for Italy. According to case law (Criminal Court of Cassation, judgement 39504/2008) the expression “subversion of the democratic order” cannot be limited to the concept of violent political action alone, but should rather refer to the Constitutional order, and therefore to any means of political struggle aimed at subverting the democratic and constitutional order or at departing from the fundamental principles governing them.

a) Crimes for the purpose of terrorism and subversion of the democratic order provided for by the Criminal Code or by special criminal laws.

In general, these are political crimes, i.e. crimes against the State's domestic and international personality, against citizens' political rights and against foreign countries, their heads and their representatives. In particular, insofar as they can be abstractly associated with the Company's activities, the following offences are recalled: "Financing of conduct for the purposes of terrorism" (Article 270-quinquies.1 of the Criminal Code), "Embezzlement of confiscated assets or monies" (Article 270-quinquies.2 of the Criminal Code), "Participation in financing the enemy" (Article 249 of the Criminal Code), "Kidnapping for purposes of terrorism or for subversion of the democratic order" (Article 289-bis of the Criminal Code) and the offence referred to in Article 270-bis of the Criminal Code, called "Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order". In particular, this last offence also concerns any type of financing of associations which intend carrying out violent acts for the purpose of terrorism or subversion of the democratic order.

Attention should also be focused on financial offences, in particular money laundering and use of money, goods or other assets of unlawful origin, naturally if such offences are instrumental to the pursuit of the aims of terrorism or subversion of the democratic order. In particular, this last offence also concerns any type of financing of associations which intend carrying out violent acts for the purpose of terrorism or subversion of the democratic order.

Attention should also be focused on financial offences, in particular money laundering and use of money, goods or other assets of unlawful origin, naturally if such offences are instrumental to the pursuit of the aims of terrorism or subversion of the democratic order.

In addition to the provisions of the Criminal Code, other relevant offences are set out in special laws covering a broad range of criminal activities (e.g. concerning weapons, drug trafficking, environmental protection, etc.) and in laws adopted in the 1970s and 1980s to combat terrorism (e.g. laws on the security of air and sea travel, etc.).

b) Crimes for the purpose of terrorism addressed by the 1999 New York Convention.

The reference to this Convention by Article 25-*quater*, paragraph 4, of the Decree clearly aims at avoiding any gaps as its intent is to further international cooperation for the suppression of the fund collecting and financing in any form to be used for terrorist activities in general or in sectors and concerning methods that entail a greater risk, which are the object of international treaties (air and maritime transport, diplomatic representations, nuclear, etc.).

Section II - Organised crime offences

Article 24-ter of the Decree, inserted by Law No. 94/2009, firstly sets out a group of offences relating to the various forms of criminal organisations, namely:

- Generic Criminal association (Article 416 of the Criminal Code, paragraphs 1 - 5);
- Mafia-type criminal association – including foreign organised crime association – and vote exchange in elections (Articles 416-bis and 416-ter);
- Criminal association for the purpose of committing the crimes relating to slavery, human trafficking and the smuggling of migrants (Article 416 of the Criminal Code, paragraphs 6 and 7);
- Association for the purpose of illicit trafficking in narcotic or psychotropic drugs (Article 74 of Presidential Decree 309/1990).

With reference to the types of criminal association listed above, it should be noted that the offence consists in promoting, establishing and participating in a criminal association consisting of three or more persons, and is therefore punishable per se regardless of whether or not the crimes pursued by the association are actually committed (any such crimes being punished separately). Consequently, the intentional participation of a representative or employee of the entity in a criminal association might of itself give rise to the entity's administrative liability, provided, of course, that participation in or support for such criminal association is also in the entity's interest or gives an advantage to it. Moreover, the association must involve at least some form of stable organisation and a common plan to carry out an indefinite series of crimes. In other words, an occasional agreement for the commission of one or more specific crimes does not constitute the offence of criminal association. Under case law moreover, the offence of aiding and abetting a criminal association is committed by a person who, while not being a member of such association, contributes in a significant manner, albeit occasionally, to its existence or to the pursuit of its objectives.

The mafia-type criminal association (Article 416-bis of the Criminal Code) differs from the generic criminal association in that its participants exploit the intimidating power of their association and the resulting condition of submission and silence to commit crimes or – even without committing crimes, yet by use of the mafia method – to directly or indirectly acquire control over economic activities, concessions, authorisations, public contracts and services, or to obtain unlawful profits or advantages for themselves or for others, or with a view to preventing or limiting the freedom of vote, or to obtain votes for themselves of for others on the occasion of an election.

This provision also applies to the "camorra" and other criminal organisations, howsoever named, including foreign crime syndicates, possessing the above-mentioned mafia-type

characteristics. The crime of vote exchange in elections is committed by a person who proposes or accepts the promise to procure votes with the use of mafia methods against the payment or the promise of money or other benefits.

Lastly, the other two types of criminal association (Article 416, paragraphs 6 and 7 of the Criminal Code and Article 74 of Presidential Decree 309/1990) are characterised by their being set up to pursue specific crimes, namely: respectively, the offences relating to reducing into slavery, human trafficking and the smuggling of immigrants, organ trafficking, sexual crimes against minors and the offences of unlawful production, trafficking or possession of drugs of abuse or psychotropic substances. Some of these specific purpose-oriented offences are in themselves autonomous predicate offences giving rise to the Entity's liability, as discussed in greater detail below, in the section on crimes against the person and transnational crimes.

Article 24-ter also includes the generic category of any type of crime committed using mafia methods or in order to further the activity of a mafia-type association; in this case too, the Entity can be held liable only where the crime was aimed at pursuing its interest or giving it an advantage.

The first circumstance occurs when the perpetrator, while not belonging to the criminal organisation or aiding and abetting it, engages in specific intimidating conduct, for example making threats by exploiting the "reputation" of criminal organisations operating in a specific territory. The case of an offence furthering the activity of a mafia-type association occurs when the perpetrator acts with this specific aim in mind and his conduct is likely to achieve the intended result, for example where a money laundering offence is committed in the awareness of the fact that the operation concerns a mafia-type organisation.

Lastly, Article 24-ter also refers the following offences, which are usually, albeit not necessarily, committed by criminal organisations.

Kidnapping for ransom (Article 630 of the Criminal Code)

The offence consists of kidnapping a person in order to secure for oneself or others unlawful gain in exchange for release of the kidnapped person. The benefit may also consist in a non-financial advantage. In particular cases, this offence might also apply to persons who did not take part in the kidnapping but took steps to ensure that the kidnappers would obtain the ransom, by contributing to the lengthening of the negotiations and consequently of the kidnapped person's deprivation of liberty, or by helping the kidnappers obtain the ransom. Moreover, the offence of money laundering could apply to any persons playing a role in the transfer, circulation or use of sums of money or other goods, knowing that such sums were obtained through the offence in question.

Crimes relating to weapons and explosives (Article 407 paragraph 2, point a), No. 5 of the Code Of Criminal Procedure)

These are offences laid down by the special laws on the subject (in particular Law No. 110/1975 and Law No. 895/1967), which punish the unlawful manufacturing, introduction into the country, sale, supply, possession and unauthorised carrying of explosives, weapons of war and common firearms, with the exception of firearms used on shooting ranges, and of gas or compressed-air firearms. In this case too, similarly to the previous offence, any type of collusion by the Company operators with the perpetrators of such offences, or the performance of activities such as, for instance, the granting of financing, with the awareness of favouring such offences, even merely indirectly, could give rise to the offence of aiding and abetting such crimes, or to other offences, e.g. money laundering.

Section III - Transnational offences

The liability of Entities for this category of offence is laid down in Law No. 146/2006, in order to enhance the effectiveness of the fight against transnational organised crime.
An offence is considered to be transnational and is punished with a term of imprisonment of not less than four years, where it involves an organised criminal group and:

- was committed in more than one Country, or
- was committed in one Country, but a significant part of its preparation, planning, management or control took place in another Country, or
- was committed in one Country, but involved an organised criminal group which pursues criminal activities in more than one Country;
- was committed in one Country, but had significant impact in another Country.

We describe below the criminal offences which may give rise to the Entity's liability where the twofold conditions of the entity's interest or advantage and of the translational nature of the crime (of which the offender must have been aware) are met.

Criminal associations under Articles 416 and 416-bis of the Criminal Code criminal associations for the smuggling of foreign tobacco products (Article 291-quater of Presidential Decree No. 43 of 23 January 1973) or to the illicit trafficking of narcotic drugs or psychotropic substances (Article 74 Presidential Decree No. 309 of 9 October 1990)

The basic characteristics of the conduct constituting criminal association are described above in the paragraphs on criminal association offences. We believe that, where such offences are of a transnational nature, the only penalties that might be applicable to the entity are those set out in Law No. 146/2006 but not those set out in Article 24-ter of the Decree.

Offences relating to the smuggling of migrants (Article 12, paragraphs 3, 3-bis, 3-ter and 5 of Legislative Decree No. 286 of 25.7.1998) [48]

Article 12 punishes the illegal transport of foreigners into the territory of the State, as well as the promotion, coordination, organisation or financing of such transport, and other acts aimed at facilitating the illegal entry of foreigners into the territory of Italy or of another country different from their country of origin or habitual residence. However, at least one of the five conditions listed in the Article must be met for this offence to take place[49].

The punishment is increased where at least two of the above-mentioned conditions are met at the same time, or where the acts were committed for specific aims such as: the recruitment of persons to be destined for prostitution; the exploitation of minors, or, in general, in order to obtain a profit, even indirectly.

Lastly, paragraph 5 punishes complicity in the permanence of a foreigner in order to obtain an unfair gain from such foreigner's illegal status. Unfair gain is deemed to occur when the balance of services is altered as a consequence of the fact that the offender is aware of the foreigner's illegal status and exploits to his advantage.

Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

This offence occurs when anyone uses violence or threats, or offers or promises money or other benefit to induce not to make statements, or to make false statements any person

[48] Crimes in the area of illegal immigration, even if they lack the characteristics of transnationality, entail liability under Legislative Decree No. 231/2001, as of 19 November 2017, the date of entry into force of Article 25-*duodecies*, paragraph 1-*bis*, of the Decree, introduced by Law No. 161/2017.

[49] In brief: a) the act concerns the illegal entry or residence in Italy of five or more persons; b) the smuggled persons' life or safety were endangered; c) the smuggled persons were subjected to inhumane or degrading treatment; d) the act was committed by three or more persons acting in association with one another or utilising international transport services or documents that are forged or altered or were in any way illegally obtained; e) the act was committed by persons possessing arms or explosives.

who is called before the judicial authorities to make statements in connection with criminal proceedings if such person has the right to remain silent.
This offence can entail the Entity's liability even where the transnational element is absent, since it is referred to not only by Law No. 146/2006, but also by Article 25-decies of the Decree.

Aiding a fugitive (Article 378 of the Criminal Code)

This offence consists of helping the author of a crime punishable by life imprisonment or a prison sentence – after the deed, and without having aided and abetted its commission – to avoid investigation by the authorities or arrest. The offence occurs even if the person so assisted cannot be charged with the crime or is found not to have committed it. The penalty is increased when the crime in question is that of participation in a mafia-type association. It should be noted that according to prevailing case law, this offence is also committed by those who give false replies on being questioned by the Judicial authorities.

Section IV - Crimes against the person

Article 25-*quinquies* of the Decree lists certain offences against individuals set out in the Criminal Code in order to forcefully combat new forms of slavery such as prostitution, human trafficking, the exploitation of children and forced begging, which are all activities strongly associated with the spread of organised crime and new criminal organisations.
In particular, the following types of crimes are identified: "Enslaving or keeping persons enslaved" (Article 600 of the Criminal Code), "Child prostitution" (Article 600-bis of the Criminal Code), "Child pornography" (Article 600-ter of the Criminal Code), "Possession of pornography material" (Article 600-quater of the Criminal Code), "Tourism initiatives aimed at exploiting child prostitution" (Article 600-quinquies of the Criminal Code), "Solicitation of minors" (Article 609-undecies of the Criminal Code), "Human trafficking" (Article 601 of the Criminal Code), "Purchasing and selling slaves" (Article 602 of the Criminal Code).
Lastly, it should be noted that Article 25-*quater* paragraph 1 provides for the administrative liability of the Entity for the crime referred to in Article 583-bis of the Criminal Code (Female genital mutilation practices).
The risk of the entity being liable for the above-mentioned crimes can only be deemed to be significant in the event that a Company representative or employee acts in conspiracy with the material author of the offence.
The following offences can also be included in this section:

- "Employment of foreign nationals with irregular permits of stay" (Article 22, paragraph 12-bis, Legislative Decree No. 286/1998 – Consolidated Law on Immigration, which is

mentioned in Article 25-duodecies of the Decree[50]), which punishes employers that hire or make use of non-EU employees without a regular residence permit, or with a permit that has expired without requesting renewal, or has been revoked or cancelled. Corporate liability for this offence, which is connected to the exploitation of illegal workers illustrated in the previous section, is only envisaged in certain aggravated circumstances[51];

- "Illegal intermediation and exploitation of labour" (Article 603 of the Criminal Code, as recalled in Article 25-quinquies of the Decree[52]) which punishes those who take advantage of the workers' needy status and intermediate, use, hire or employ labour under conditions akin to exploitation. Situations such as the payment of remuneration that does not align with the labour union contracts, repeated violation of the working hours and rest regulations, violation of the occupational health and safety regulations are included among the exploitation indices;
- "Racism and xenophobia" (Article 604-*bis*, paragraph 3 of the Criminal Code, as recalled in Article 25-*terdecies* of the Decree), which punishes the instigation, provocation or propaganda that promote discrimination, or racial, ethnic, national or religious violence based on the denial or trivialization of the Holocaust or other crimes of genocide, war, or against humanity.

Section V - Offences relating to fraud in sporting competitions, illegal betting or gaming

Article 25-*quaterdecies* of the Decree refers to offences relating to fraud in sporting competitions, illegal betting or gaming. The offence of sports fraud is committed by anyone who offers or promises cash or other benefits or advantages to any participants in a sporting competition organised by a recognised federation, or who commits other acts of fraud for the same purpose. The same article also refers to offences and contraventions relating to the exercise, organisation or sale of lotteries, betting and gaming and the use of gaming machines in the absence of or in breach of the required licences or concessions.

7.5.2 Sensitive company activities

In the banking industry, the risk of offences being committed for the purposes of terrorism or subversion of the democratic order, or the risk of organised crime, transnational offences, offences against the person and offences relating to fraud in sporting

[50]Article 25-duodecies was inserted into Legislative Decree No. 231/2001 by Article 2 of Legislative Decree No. 109/2012, effective from 9.8.2012.
[51] One of the following circumstances has to exist: a) employment of more than three workers without regular permits; b) exploitation of minors without regular permits; c) exposure to situations of extreme danger.
[52] The reiteration of Article 603-bis was added to Article 25-quinquies of the Decree by Article 6 of Law No. 199/2016, which is in effect from 4.11.2016.

competitions, the illegal exercise of betting or gaming, mainly relates to, in the scope of the Company's activity, the activities of establishing relations with customers connected with the transfer of funds, as well as the performance of instrumental or related activities, activities which, for the purposes of preventing the offences in question, must be based on the fundamental principle of adequate knowledge of customers. This principle represents one of the key requirements established by Legislative Decree No. 231/2007 concerning prevention of the use of the financial system for the purpose of money laundering and of financing terrorism.

The activities identified above are those where the risk of money laundering offences is also higher. Therefore, for the purposes of preventing the offences illustrated above, the control and conduct principles identified in the protocol “Financial fight against terrorism and money laundering” are deemed appropriate.

Furthermore, the offences in this section also include:

- “*inducement to withhold information or to make false statements to the judicial authorities*”; the company activity considered to be most sensitive in this respect is the management of disputes and settlements;
- “*employment of foreign nationals with irregular permits of stay*”, and “*Illegal intermediation and exploitation of labour*”: sensitive activities regarding the former category are those pertaining to the recruitment and hiring of personnel, and for both categories, procedures relating to the purchasing of goods, services and consulting contracts.

Reference is therefore made to the protocols set out respectively in Chapter 7.2.2.4 for the "Management of disputes and settlement agreements", Chapter 7.4.2.1 for the "Financial fight against terrorism and money laundering", Chapter 7.2.2.8 for the "Management of the staff selection and recruitment process" and 7.2.2.6. “Management of the procedures for the procurement of goods and services and for the appointment of professional consultants”.

Such protocols also apply to the monitoring of any activities performed by Group companies and/or outsourcers on the basis of special service agreements.

7.6 Sensitive area concerning crimes and administrative offences relating to market abuse

7.6.1 Type of offence

The Finance Consolidation Act provides for the offences of "*insider dealing*" and "*market manipulation*", regulated in Articles 184 and 185 respectively.

Articles 187-*bis* and 187-*ter* of the Finance Consolidation Act include the administrative offences of "*abuse and disclosure of insider information*" and of "*market manipulation*", for which the illegal acts are essentially the same as for the previous two offences.

The responsibility of the Entity in whose interests these two criminal offences were committed is punished by Legislative Decree No. 231/2001 (Article 25-*sexies*), while for the two administrative offences, the responsibility derives from the Finance Consolidation Act (Article 187-*quinquies*) which is based on the same principles, conditions and exemptions as Legislative Decree No. 231/2001, except that for these administrative offences, the Entity will be liable whenever it is unable to provide proof that the perpetrator of the offence acted only in his or her interests or in the interests of a third party.

It should also be recalled that the offence of market abuse in the broad sense also includes the offence of market rigging (placed among corporate offences: see paragraph 7.3.1), which concerns financial instruments that are not listed or for which no application for admission to trading on a regulated market has been made.

The above-mentioned rules are aimed at ensuring the integrity, transparency, correctness and efficiency of the financial markets, in accordance with the principle that all investors should operate on a level playing field with regard to access to information, knowledge of the pricing mechanism and knowledge of the source of publicly available information.

The rules for the implementation of this principle and for the punishment of its violations are laid down in European Union legislation, most recently with Directive 2014/57/EU (the so-called MAD II) and with Regulation (EU) No. 596/2014 (the so-called MAR); and by the Italian legal system with Legislative Decree No. 107/2018, in force since 29 September 2018, which also rewrote the sanctioning provisions of the Finance Consolidation Act mentioned above. Except for what is specified below with reference to each of the various offences, the punishable conduct may relate to[53]:

1) financial instruments admitted to trading or for which an application has been submitted for admission to trading on a regulated Italian or other EU market;

[53] Under Article 183 of the Finance Consolidation Act, the regulation of market abuses does not apply to monetary management and public debt activities, nor activities relating to climate policy, nor to own-share buyback schemes or schemes to stabilise securities prices, in accordance with the rules in Article 5 MAR.

2) financial instruments admitted to trading or for which an application has been submitted for admission to trading on a multilateral trading facility (so-called MTF) in Italy or of another European Union country;
3) financial instruments traded on an organised trading facility (so-called OTF) in Italy or of another European Union country;
4) other financial instruments not covered by the previous points, traded outside the aforementioned trading venues (so-called OTC), or whose price depends on or has an effect on the prices of instruments traded on the venues referred to in the preceding numbers, including credit default swaps and contracts for differences;
5) spot commodity contracts as defined by MAR;
6) benchmarks as defined by MAR;
7) EU-wide trading of greenhouse gas emission allowances or other related products traded on authorised auction platforms, pursuant to EU Regulation No. 1031/2010.

Under Article 182 of the Finance Consolidation Act, the offences are punishable under Italian law even if committed abroad, where these offences involve financial instruments admitted to trading, or for which admission to trading has been requested, on an Italian regulated market or on an Italian MTF, or if they relate to financial instruments traded on an Italian OTF.

Under Article 16 of the MAR, market operators and investment firms who manage a trading facility and who prepare or execute trading operations on a professional basis are required to adopt effective systems, devices and procedures[54] to prevent, identify and immediately report any suspicious orders or transactions to the relevant authorities, if they could amount to insider trading or market manipulation, or even attempts at such offences.

The violation of these obligations is regulated by Article 187-ter.1 of the Finance Consolidation Act; A failure to report any violations may, in theory, expose the Company to involvement in the offence committed by the customer, depending on the circumstances and methods surrounding the operation.

A description of the above cases is given below.

Abuse or unlawful communication of inside information, recommendation or inducement of others to commit insider dealing (Article 184 Finance Consolidation Act)

This offence punishes anyone who directly or indirectly misuses inside information they have received (i) because they are a member of the Board of Directors, management or control body of the issuer; (ii) because they participate in the capital of the issuer; or (iii)

[54] The reporting procedures are defined by CONSOB in Article 4-*duodecies* of the Finance Consolidation Act, in accordance with the rules on internal whistleblowing systems.

because they hold a position or function in relation to their working or professional activities; (iv) as a result of the preparation or commission of a crime (e.g. " *intrusion into a computer system and extraction of inside information* ").

Any of the above-named persons commits an offence if[55]:

a) who buys, sells or carries out other operations[56] on financial instruments either directly or indirectly on their own account or on behalf of a third party, using that information (insider trading);

b) discloses that information outside of the normal exercise of their work or professional or outside of a market survey in accordance with Article 11 (tipping);

c) recommends to, or induces other people to carry out any of the above operations, on the strength of that information (tuyautage).

Inside information means information of a "*specific nature which has not been made public*[57]*, relating, directly or indirectly, to one or more issuers of financial instruments or one or more financial instruments, which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments or on the prices of related derivative financial instruments*[58]".

Insider information may also relate to: i) commodities derivatives; ii) related spot commodity contracts; iii) greenhouse gas emissions allowances or other related products; iv) information provided by the customer in connection with pending orders in the customer's financial instruments, which if made public may have a significant effect on the prices of such instruments, on the connected spot commodity contracts or on the connected derivatives.

The conduct shall be punished less severely, as a misdemeanour, where the transactions do not concern Italian or EU regulated markets, but the financial instruments referred to in Nos. 2), 3) and 4) above, as well as the exchange of units referred to in No. 7.

Within the specific scope of the Company's operations, there are various cases that could entail the liability of the Asset Management Company in the event that the offence is committed in its exclusive or concurrent interest. The risk is conceivable when the person who arranges or executes the transaction misuses inside information concerning a particular issuer to which the Company has access in the course of its Fund management activities (by virtue, for example, of taking a stake in the issuer's capital). A special case

[55] Article 184 of the Finance Consolidation Act does not punish the so-called secondary insider, i.e. the person who has obtained inside information in circumstances other than those listed, e.g. the person who uses the information communicated to him or her, even without recommendation or inducement, by a qualified person.
[56] This also includes operations to cancel or amend a previous order that was given before having access to the inside information.
[57] Article 17 MAR provides for the cases, times and terms regarding the obligation on the part of the issuer of financial instruments or participants in the market for greenhouse gas emissions quotas, to disclose insider information to the public.
[58] The definition of inside information is established by Article 180, paragraph 1, letter b-ter of the Finance Consolidation Act, by simple reference to Article 7, paragraphs 1 to 4 of the MAR. Reference should be made to this provision for a detailed reconstruction, in particular regarding the concepts of "precise nature" and "significant effect".

may exist where a member or employee of the Company is a member of executive bodies in other companies, and exploits insider information obtained from the other company, in the interests of the Company.

Market manipulation (Article 185 of the Finance Consolidation Act)

The offence of "*market manipulation*" is committed by anyone who spreads false news or carries out simulated transactions or other artifices that are concretely likely to cause a significant alteration in the price of financial instruments[59].

There is no punishment for orders for sale and purchase or other operations which, although having the potential to give misleading signals to the market or to artificially set the price, are justified by legitimate reasons and which were carried out in accordance with market practice permitted by the regulator responsible for the reference market according to Article 13 of the MAR.

The conduct is punished less severely, as a misdemeanour, where the transactions do not concern Italian or EU regulated markets, but the financial instruments referred to in Nos. 2), 3) and 4) above, as well as the exchange of units referred to in No. 7.

The conduct is also punishable if it concerns:

- spot commodity contracts which are not wholesale energy products, if the facts are capable of causing a significant alteration in the price or value of the financial instruments specified in numbers 1) to 4) above, or those financial instruments, including derivative contracts or derivatives for the transfer of credit risk, if the facts are capable of causing a significant alteration in the price or value of a spot commodity contract, where that price or value depends on the prices or values of those financial instruments;
- benchmarks, as defined in Article 3, paragraph 1, No. 29 of the MAR.

In the context of the Company's typical operations, the risk of commission of the offence in question is deemed conceivable in the event of so-called manipulation of information (for example, through the distorted use of marketing communications or other information, including commercial and promotional information, concerning issuers of financial instruments and/or listed financial instruments).

Administrative sanctions: insider trading and market manipulation (Article 187-bis and Article 187-ter Finance Consolidation Act)

As stated above, specific administrative sanctions have been introduced to punish the same material acts which give rise to both types of criminal offence (Articles 184 and 185 of the Finance Consolidation Act).

[59] For a more detailed description of the operations and systems that can give false or misleading information to the market or which set the market price at an irregular level, see Article 12 and Annex I of the MAR, which contains a non-exhaustive list of indications of manipulation consisting of the use of false or misleading information, in price setting and in the use of false instruments or other devices.

The administrative offences governed by Articles 187-*bis* and 187-*ter* of the Finance Consolidation Act do not describe the prohibited conduct but simply refer to the prohibition on the abuse or unlawful disclosure of insider information and market manipulation, as defined in Articles 14 and 15 of the MAR[60]. The reference to the definitions of the cases contained in European legislation also entails a generic reference to the other MAR provisions that define the concepts of abuse, illegal communication and manipulation, and which are also the reference source for the crimes illustrated above, even though no express reference is made.

The cases of administrative offence, the application of which falls within the competence of Consob, could therefore affect a broader range of conduct[61], insofar as the elements and modalities taken up through direct reference to Articles 14 and 15 of the MAR (and consequently to the rules of the MAR itself that constitute its prerequisites) are considered relevant, and not so for the criminal conduct, which has been described without express reference to the MAR except for circumscribed aspects.

Another factor that could lead to a more extensive and incisive application of administrative penalties than criminal penalties is the fact that, whereas for the criminal offence it is necessary to prove intent, for the administrative offence negligence is sufficient.

This does not rule out the possibility of the same person being prosecuted and punished for the same acts, with cumulative proceedings and punishments for the crime and for the administrative offence: in such a case, Article 187-*terdecies* of the Finance Consolidation Act provides that the legal authorities and Consob need to take into account – when issuing the penalties against the individuals who committed the offences and the entities who are liable for the criminal and administrative offences committed by their employees or executives – any sanctions already imposed during the criminal or administrative proceedings that were concluded first, and that in any case the second fine may only be imposed for the amount in excess of the first fine[62].

7.6.2 Sensitive company activities.

The sensitive activities identified by Model which involve the highest risks of crimes and administrative offences relating to market abuse are the following:

[60] The liability of the entity for the administrative offence committed by its employees or top management is also indicated in Article 187-*quinquies* of the TUF by referring to the violation of the prohibitions referred to in Articles 14 and 15 of the MAR. A pecuniary sanction from €20,000 to €15 million is envisaged for the entity, or up to 15% of turnover, if this is greater than €15 million. The punishment will be increased to up to ten times the product or proceeds of the offence, if of a large amount. In addition, the product or proceeds of the administrative offence will be confiscated.

[61] For example, the conduct of the secondary insider is not punishable under Article 184 of the Finance Consolidation Act, but is instead punishable under Article 187-*bis*, by virtue of the full reference to Article 14 of the MAR.

[62] The entity may thus be liable both for the administrative offences or crimes, and for the criminal offences charged to an employee, for the same events. The sanctions imposed on the entity for the administrative offences indicated in the above note could thus be added to the punishment for criminal offences as provided for in Article 25-*sexies* of Legislative Decree No. 231/2001, namely a fine of up to €1,549,000, increased up to ten times the product or proceeds that were obtained, if of a large amount.

- Management and disclosure of information and of external communications for the purposes of prevention of criminal and administrative offences in the area of market abuse;
- Managing orders and market transactions to prevent administrative and criminal offences linked to market abuse.

We reproduce below, for each of the above-mentioned sensitive activities, the protocols laying down the control principles and rules of conduct applicable to these activities, as well as the detailed corporate regulations governing such activities.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.6.2.1 Management and disclosure of information and of external communications for the purposes of prevention of criminal and administrative offences in the area of market abuse

This protocol applies to all members of corporate bodies and employees of the Company who have access to inside information, within the meaning of the laws and regulations in force.

The process of managing and handling inside information could present opportunities for the commission of the offence of insider trading or the related administrative offence, provided for respectively in Articles 184 and 187-bis of the Finance Consolidation Act.

Sound management of this process also goes to prevent the offences of market rigging and market manipulation and their corresponding administrative breach – respectively set out in Article 2637 of the Civil Code and in Articles 185 and 187-ter of the Finance Consolidation Act – with regard to “information manipulation”, ensuring adequate control of the potential risk of “dissemination of false or misleading information, rumours or news”.

According to CONSOB's guidelines, for the Asset Management Company, as an entity controlled (albeit indirectly) by a listed issuer, information that can be considered of a privileged nature for the listed parent company in light of the subsidiary's significance is also relevant. In relation to the above, it is acknowledged that the information relating to the Company is not normally such in terms of significance as to entail effects capable of influencing the Parent Company's share price. Therefore, in order to ensure adequate awareness of all personnel, the control and behavioural principles adopted by the Parent Company, transposed by the Company, aimed at ensuring compliance with the relevant primary and secondary legislation in force and the principles of confidentiality of the information processed and secrecy in the handling of information not in the public domain, are also set out below.

The purpose of the rules set out in this document, in compliance with the requirements of current legislation, is to ensure that:

- the circulation of information in the corporate context may take place without prejudice to the privileged or confidential nature of such information and avoid the sharing of such information with unauthorised parties;
- inside information is not disclosed, even unintentionally, to third persons for reasons not related to the office activity, prescribing to this purpose a particularly cautious conduct to the members of the Corporate Bodies, employees or other persons involved, as well as obligations to report to the competent Company Structures any situations which may entail the risk of unauthorised disclosure of such information;

- members of the Corporate Bodies and persons involved in the Company's operations do not misuse inside information, which they possess by virtue of the role they hold and/or the functions they perform within the company, to trade in financial instruments in the interest of or on behalf of the Company and/or for personal reasons;
- ensure the timely disclosure to the Parent Company of inside information concerning the Company if it has a material impact on the Parent Company or the Group as a whole; this is to ensure the timely disclosure of such information to the market[63].

The Intesa Sanpaolo SpA Group Regulation for the management of inside information implemented by resolution of the Company's Board of Directors, provides for the adoption of internal organizational measures aimed at the management and timely disclosure to the public of inside information concerning it directly, in compliance with the provisions in Articles 17 and 18 of the MAR. In particular, the organizational, management and control measures of inside information are aimed at ensuring conditions of correctness, efficiency and timeliness in the transparency of the Parent Company's disclosure, as well as the methods of handling information that could have a significant effect on the prices of the financial instruments issued by the same and traded on relevant markets or even on the prices of related derivative financial instruments.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The process of managing and disclosing the inside information of which the Company's structures become aware is organised in accordance with the specific operational responsibilities assigned under the Company's role and task allocation system.

The criteria used for identifying inside information and relevant information (as defined in the Consob Guidelines of 13 October 2017 on the management of insider information), and the operating procedures for managing that information are governed by the internal rules developed and updated by the competent Structures which form an integral and substantial part of this protocol.

By reason of their operational duties and functions within corporate operations, the Company's structures may handle inside information concerning:

- the Company itself, if such information has a material impact on the financial performance of the Parent Company or the Group as a whole;

[63] This fulfilment is due as the Company is controlled by a listed issuer that is bound by specific disclosure obligations towards the market in order to avoid information asymmetries among the public.

- investee companies of the funds managed by the Asset Management Company and the financial instruments issued by them (inside information on third-party issuers);

and which are of a precise nature, which have not been made public and which relate, directly or indirectly, to one or more issuers of financial instruments or to one or more financial instruments, and which, if made public, would be likely to have a significant effect on the prices of those financial instruments or on the prices of related derivative financial instruments.

The specific relevant information and privileged information are identified on the basis of the criteria set out in the relevant internal or Group regulations and, by way of example, may arise from an internal Company decision (e.g. strategic initiatives, agreements and extraordinary transactions) or derive from the ascertainment of objective events or circumstances having an impact on the activity of the company, the Parent Company or the Group as a whole and/or on the price of the financial instruments issued (e.g. accounting situations for the period, management news). In addition, inside information may arise from events and circumstances relating to companies issuing financial instruments in which the Funds managed by the Company invest.

Inside information relating to third-party issuers or financial instruments issued by them may also derive from operations relating to both investment services and activities, and activities on the primary market and ancillary services (corporate finance, in particular such as advisory services, M&A and extraordinary transactions concerning the issuer's capital or debt structure, etc.) when provided to issuers of listed financial instruments, or to issuers of financial instruments for which admission to trading on a regulated market has been requested, or issuers of financial instruments. admitted to trading on an MTF or OTF, or for which a request for admission to trading on an MTF has been submitted.

In the absence of specific regulatory obligations and in line with the principles defined by the Parent Company, the Company has voluntarily established a register of persons with access to inside information relating to third-party issuers (appropriately regulated in internal regulations) in order to ensure the traceability of access to inside information in the context of UCITS management activities.

With regard to the Company's own inside information of relevance to the Parent Company or the Group as a whole, the process of disclosing price-sensitive information to the market consists of the following stages:

- identification of inside information by the Chair of the Board of Directors and the Chief Executive Officer;
- timely reporting of such information to the competent structure of the Parent Company;

- communication, well in advance of the deadline required by the fulfilment of disclosure obligations, of any element necessary to support the drafting of press releases by the competent structure of the Parent Company;
- approval of the text of the press release referring to the information provided by the Company.

All such measures are defined and regulated in greater detail in the internal procedures, policies, and regulations in force from time to time, which form an integral and substantial part of this protocol.

Control principles

With regard to aspects related to the possession of inside information on third-party issuers, the control system is based on the following factors:

- establishment of a Register of persons with access to inside information relating to third-party issuers: internal rules outline the process for maintaining and managing the Register, as well as the corporate function responsible for managing it from time to time. This function is responsible for the fulfilment of information obligations vis-à-vis persons entered in the Register and complies with access requests made by the competent authorities;
- in addition to the set-up of the Register, at least the following protection measures are taken, listed by way of example and not exhaustively:
    - no specific relevant information is to be transmitted to the employees of the structure owning the information (hereinafter SOP) unless such transmission is authorised in advance by the person in charge of the SOP who intends to transmit the information;
    - the possibility of accessing specific relevant information or inside information must be limited to anyone who needs the information to perform their work, and they must be instantly entered on the register;
    - in any case, anyone who has free access to the specific relevant information must be entered, without any further prior authorisation;
    - each member of the Structure who obtains specific relevant information or inside information accidentally, during the course of their work, is required to report this immediately to the Manager of the SOP involved who, based on the available information, will promptly register the incident and will check the robustness of the control measures within their department;
- implementation of logical and physical security systems to guarantee the proper management of information;

- adoption of functional and logistical separation measures (so-called Chinese Walls) between the different corporate Functions, assigning to the resources concerned specific profiles and qualifications for carrying out the activities;
- the obligation for persons involved in the Company's operations to immediately inform their hierarchical superior and the Compliance and AML Function of the occurrence - in relation to a specific transaction that may satisfy the requirements of a sensitive situation for entry in the Register - of situations of conflict of interest (even if only potential), on their own behalf or on behalf of third parties, arising in particular from family or marriage relationships or from their own or their relatives' financial interests: this is without prejudice to the general obligation of abstention laid down in Article 3 of the Group's Internal Code of Conduct;
- provision of rules identifying the obligations and limits to which members of the Corporate Bodies, employees and collaborators, among others, are subject when they wish to carry out investment transactions on financial instruments on a personal basis: these rules provide for specific prohibitions and restrictions for all those who are entered in the Register and who therefore hold inside information on a specific third-party issuer.

With regard to aspects related to the disclosure to the market of inside information of the Company having a material effect on the Group, the procedure is as follows:

- the Chair of the Board of Directors and the Chief Executive Officer of the Company are responsible for identifying circumstances and events that may give rise to inside information;
- at the indication of the Chair and/or Chief Executive Officer of the Company, the corporate Structures in charge are required to promptly contact the Intesa Sanpaolo Inside Information Management function (hereinafter also FGIP), in order to establish whether the Company's inside information is such as to have an impact on the Parent Company or on the Group as a whole and to ensure proper compliance with public disclosure obligations;
- the competent structures of the Parent Company prepare press releases on price-sensitive information for the Group[64]; these press releases are disseminated – subject to authorisation by the competent corporate bodies – to the relevant Supervisory Authorities, via eMarket SDIR, by Price-Sensitive Communication, which also promptly publishes them on the Parent Company's website;
- the competent structures of the Parent Company are responsible for managing relations with financial analysts, institutional investors and rating agencies in order to disclose

[64] Therefore, they also refer to events attributable to the sphere of activity of the Subsidiaries, including Neva SGR, which have a significant impact on the Group's economic and financial performance.

relevant information, ensuring its uniformity also in the event that it is disseminated externally via the Internet.

Rules of conduct

The Corporate Structures, as well as each employee or collaborator, which are howsoever involved in management and disclosure of privileged information shall comply with the procedures set out in this protocol, the applicable provisions of law, the internal and Group rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

Specifically:

- all the information and documents acquired in the course of discharging one's duties, whether concerning the Company or other companies of the Group, or concerning third party companies in which the funds managed or which have a business relationship with the Company and their financial instruments shall be kept confidential; all such information or documents shall be used exclusively in discharge of work-associated duties;
- it is forbidden to carry out transactions on financial instruments of the Parent Company and of third-party companies in which the funds managed invest or which have a business relationship with the Asset Management Company, in relation to which inside information on the issuer or the security itself is possessed, knowing or being able to know on the basis of ordinary diligence the privileged nature of the information, especially where separation measures (Chinese Walls) envisaged for this purpose were not sufficient to prevent the circulation of the information itself or specific restrictions were arranged. This prohibition applies to any type of transaction in financial instruments (for example: shares, bonds, warrants, covered warrants, options, futures);
- specific relevant information and inside information may be disseminated within the corporate Structures of the Company or the outsourcer only to those who have an actual need to know such information for reasons relating to the normal performance of their duties, highlighting the confidential nature of the information and making such dissemination known for the purpose of entering the persons concerned in the Register of persons with access to inside information. Furthermore, in the event that a person entered in the Register involuntarily discloses inside information to another person who is not authorised to access it, the person who inadvertently made the disclosure must report the event to the Compliance and AML Function for the necessary action;
- it is forbidden to disclose inside information to third parties for any reasons other than performance of duties and in any case where they are not bound to comply with a documentable obligation of legal, regulatory, statutory or contractual non-disclosure, as they are required to arrange for the immediate signing of specific non-disclosure

agreements, with particular regard to the relations with counterparties. In any case, the selective disclosure to third parties of the specific relevant information and inside information is only permitted if all the necessary precautions and measures have been taken to avoid its improper internal or external disclosure. The obligation to enter all persons, individually and even if they belong to the same Company, in the Register of Persons in Possession of Inside Information remains unaffected;

- it is prohibited to advise or induce third parties to carry out transactions linked to the inside information;
- it is forbidden to discuss inside information in public places or in premises where persons not belonging to the company are present or in any case in the presence of persons who do not need to know such information. For example: no inside information can be discussed in open spaces with various facilities, lifts, hallways, snack areas, company canteens, restaurants, trains, airplanes, airports, buses and, in general, places accessible to the general public; special attention must also be paid when using cell phones and loudspeaker phones;
- without prejudice to the provisions on public disclosure of inside information of the Company having an impact on the Parent Company or the Group to which it belongs, it is forbidden to disclose to the market or to the media inside information relating to the companies in which the funds managed are held. If comments on specific transactions concerning such issuers are requested, any comments made shall refer only to facts already disclosed by the issuer under Article 114 of the Finance Consolidation Act; in any case, the Company staff member concerned has an obligation to consult with the corporate functions that lawfully hold the inside information to enable them to check whether confidential information has also been inadvertently disclosed;
- it is forbidden to disseminate, both to other personnel and outside the Company, through any information channel, including the Internet, information, rumours or news that do not correspond to reality, or information whose truthfulness is not certain, capable, or even only potentially capable, of providing false or misleading information on the Company or the Group and/or the relevant financial instruments, as well as in relation to third-party companies in which the funds managed invest or with which the Company has a business relationship and the relevant financial instruments;
- it is forbidden to produce and disseminate studies and researches in infringement of the internal and external rules specifically laid down for such activity and, in particular, without ensuring that the information provided is clear, accurate and not misleading, without disclosing in the manner required by law the existence of any significant interests and/or conflicts of interest. It is also mandatory to prepare all documents containing

assessments such as the fairness opinion, public recommendation and formal valuation, on the basis of objective elements (financial statements, market practices, financial models, etc.);

- in accordance with the provisions of the internal rules on physical and logistical security all documents containing confidential and reserved information must be filed securely: to this end, staff members shall take care to maintain their own personal password secret and shall ensure that their computer is adequately protected, and that access to it is temporarily blocked wherever they move away from their workstation. Also note that:
  - the activity of producing documents (such as, for example, printing and photocopying documents) containing inside information must be supervised by personnel already in possession of such information;
  - the documents in question shall be classified as “confidential”, “reserved” or, where possible, using code names to safeguard the kind of information they contain; when confidential and reserved information is prepared/processed/transmitted/filed in electronic format access to such information shall be password protected or, for those Structures so equipped, will involve the use of encryption software;
  - the physical supports containing confidential and reserved information must be kept in secure controlled-access premises, or placed in controlled or protected archives after their use, and must never be left unattended, especially when they are taken outside the workplace;
  - destruction of the physical supports containing confidential and reserved information must be carried out by the same persons responsible for them, using appropriate procedures to avoid any unauthorised retrieval of the information they contain.

  Furthermore, with particular regard to the issue of official communications to the market, such communications shall be prepared in compliance with the applicable laws and regulations and, in any case, fully respecting the requirements of correctness, clarity, and equal access to the information, according to the methods and competences defined by the Group's rules, where:
  - correctness means exhaustive and non-misleading information, having regard to the legitimate requests for data and news coming from the market;
  - clarity refers to the forms in which the information is communicated to the market and means that it must be complete and clearly understandable, also taking into account the intended recipients of the communications;
  - equal access means that no information that might be relevant for assessment of financial instruments may be communicated in any manner that is howsoever selective. The case in point also includes the unintentional dissemination of

privileged information for which company regulations anticipate an immediate notification of the event to the competent function to allow the timely dissemination of the press release in accordance with the procedure relative to communicating price sensitive information to the market;

- the disclosure of inside information to the Supervisory Authorities shall take place in an exhaustive, timely and appropriate manner, in compliance with the applicable rules and regulations. Prior to this communication no declaration concerning inside information may be released to external parties.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.6.2.2 Managing orders and market transactions to prevent administrative and criminal offences linked to market abuse

This protocol applies to all the Company Structures involved in the management of market transactions on financial instruments.

The process of managing market transactions presents potential opportunities for commission of the offences of market rigging and market manipulation or the corresponding administrative breach, covered respectively by Article 2637 of the Civil Code, and by Articles 185 and 187-ter of the Finance Consolidation Act, with reference to the conduct of "operating manipulation".

With regard to the prevention of criminal and administrative offences of information manipulation – which can consist in the dissemination of false or misleading information, rumours or news – reference is made to the protocol set out in Chapter 7.6.2.1 on *"Management and disclosure of information for the purpose of preventing criminal and administrative offences relating to market abuse"*, which sets out the control and conduct principles to be observed in the process of managing inside information that could come to the knowledge of the Company's corporate Structures in the performance of their assigned duties.

The purpose of the rules set out in this document, in accordance with the requirements of current legislation, is to ensure that during execution of trading and settlement transactions on the market – or when orders to execute such transactions are given to third parties – no simulated transactions or other fictitious devices likely to have a significant effect on the prices of financial instruments are carried out, or transactions or other fictitious devices likely to provide false and misleading information on the offer, demand for, or the price of the financial instruments.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The process of managing orders and market transactions, for the purposes of this protocol, mainly concerns the activity carried out by the Company on behalf of the managed funds[65] concerning the financial instruments referred to in Article 182 of the Finance Consolidation Act. The process mainly covers the following activities:

[65] The company does not engage in market transactions on its own account.

- analysis of target companies for potential investments or management/disposal of assets already held;
- verifying compliance with the qualitative and quantitative limits imposed by the regulations of the funds managed and the possible presence of conflicts of interest;
- compliance with the approval process envisaged for the completion of the transaction;
- indirect execution on the markets of trading transactions;
- fulfilment of the administrative/regulatory requirements associated with performance of the trading transactions.

The operating methods for managing the process are governed as part of internal regulations developed and updated by the competent Structures, which constitute an integral and substantial part of this protocol.

Control principles

The system of controls for monitoring the process described is based on the following factors:

- authorisation levels defined according to the current system of powers and delegations approved by the Board of Directors with particular reference to the powers to authorise transactions relating to the Funds' investments/divestments.
- functional juxtaposition between the structures proposing the investment/disinvestment operations of the managed Funds' assets and those issuing any authorisation, in compliance with the Funds' investment policies and the limits set out in the Management Rules;
- process traceability including both the electronic and the paper trail:
    - full traceability at the document level of the process of purchase/sale of stakes/securities on behalf of the managed funds;
    - archiving and preservation of all documentation produced, by the structure concerned, in order to ensure the reconstruction of responsibilities and the reasons for the choices made;
    - audits of investment/divestment operations of the managed Funds by second- and third-level control functions; the former, in particular, carry out, for the aspects within their competence, a preventive validation activity on compliance with the internal procedures and Regulations of the managed funds, with particular reference to qualitative/quantitative aspects (risk management) and to the controls implemented on conflicts of interest and inside and confidential information (compliance).

Rules of conduct

Individuals in any capacity involved in the process of managing the funds' assets are required to apply the operating procedures set out in this protocol, the relevant existing legal provisions, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular, it is forbidden to:

- set up sham transactions or employ other fictitious devices likely to significantly affect the price of financial instruments;
- undertake transactions or issue purchase or sale orders which provide or are likely to provide false or misleading indications on the offer, demand for or price of financial instruments;
- undertake transactions or issue purchase and sale orders making it possible, also through the coordinated action of several persons, to fix the market price of financial instruments at an abnormal or artificial level;
- undertake transactions or issue purchase and sale orders employing fictitious devices or any other form of deception or contrivance;
- use other fictitious devices likely to provide false or misleading indications on the offer, demand for or price of financial instruments.

The following types of conduct concerning the financial instruments referred to in Article 182 of the Finance Consolidation Act are forbidden, with the exception of those cases and procedures set out in current legislation:

- undertake transactions or give orders to trade which represent a significant proportion of the daily volume of transaction in the relevant financial instrument on the regulated market concerned, in particular when these orders or transactions lead to a significant change in the price of the financial instrument;
- undertake transactions or give orders to trade when holding a significant buying or selling position in a financial instrument leading to significant changes in the price of the financial instrument or related derivative or underlying asset
- undertake transactions leading to no change in beneficial ownership of the financial instrument;
- undertake transactions or give orders to trade which include position reversals in a short period and represent a significant proportion of the daily volume of transactions in the financial instrument on the market concerned, and might be associated with significant changes in the price of a financial instrument;

- undertake transactions or give orders to trade which are concentrated within a short time span in the trading session and lead to a price change which is subsequently reversed;
- give orders to trade that change the representation of the best bid or offer prices in a financial instrument, or more generally change the representation of the order book available to market participants, and are removed before they are executed;
- undertake transactions or give orders to trade at or around a specific time when opening or closing auction prices, control prices, reference prices, settlement prices and valuations of financial instruments are calculated and lead to price changes which have an effect on such prices;
- execute transactions or give trading orders by preceding or following such transactions with the dissemination, including through connected persons, of false or misleading information;
- undertake transactions or give orders to trade before or after producing or disseminating research or investment recommendations which are erroneous or biased or demonstrably influenced by material interest.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.7 Sensitive area concerning workplace health and safety offences

7.7.1 Type of offence

Article 25-septies of the Decree includes in the list of the predicate offences giving rise to the liability of Entities the offences of unintentional killing (manslaughter) and of unintentionally causing grievous bodily injury where such offences are committed through violation of accident prevention and workplace health and safety rules.

The Consolidated Law on protection of health and safety in the workplace (Legislative Decree 81 of 9 April 2008), reorganised in a coherent framework the large number of previous legislative acts governing this area, with Article 30 setting out the required contents of the Organisational, Management and Control Model in this area for the purpose of preventing the offences in question.

The purpose of the above legal provisions is to provide more effective means of prevention and punishment, in the light of the spike in the number of workplace accidents and of the need to safeguard the physical and mental well-being of workers and the safety of workplaces.

The above-mentioned offences are briefly described below.

Involuntary manslaughter (Article 589 of the Criminal Code)

Involuntary serious or grievous bodily injury (Article 590 paragraph 3 of the Criminal Code)

The two offences consist in culpably causing respectively death or serious or grievous bodily harm.

Serious bodily injury indicates a condition which endangers the life of the injured person, or causes incapacity to attend to normal activities for a period exceeding forty days, or an injury which results in the permanent weakening of a sense or an organ; grievous bodily injury indicates a probably incurable condition; the loss of a sense, a limb, an organ or the capacity to procreate, permanent impairment of the power of speech, and facial deformity or permanent disfigurement.

Under the above-mentioned Article 25-septies of the Decree, to give rise to the Entity's liability, both conducts must be characterised by violation of workplace accident prevention and health and safety protection regulations.

In this regard, a large number of special laws are taken into consideration, most of which have now been incorporated into the Consolidated Law on the protection of health and safety in the workplace following the repeal by the same Consolidated Law of several special laws previously in force, including, basically: Presidential Decree No. 547 of

27.4.1955 on the subject of accident prevention; Presidential Decree 19.3.1956 No. 303 regulating occupational hygiene; Legislative Decree No. 626 of 19.9.1994 containing general rules on the protection of workers' health and safety; Presidential Decree No. 758 of 19.12.1994; Legislative Decree No. 494 of 14.8.1996 on construction site safety.

The specific prevention requirements set out in sector special legislation are complemented by the more general provision of Article 2087 of the Civil code, which requires employers to set in place measures to protect the physical and mental health of workers having regard to the characteristics of the work, the workers' experience and the techniques employed.

Lastly, it should be noted that according to case law the employer may also be liable for the offences in question where the injured person is not a worker but a third party, provided that his presence at the workplace at the time of the accident was neither anomalous nor exceptional.

7.7.2 Sensitive company activities

The protection of occupational health and safety is a requirement applying throughout all companies, areas and activities.

We reproduce below the protocol laying down the control principles and rules of conduct applicable to the management of the risks relating to workplace health and safety. This protocol is completed by the applicable detailed corporate regulations in force.

This protocol also applies to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.7.2.1 Management of the risks relating to workplace health and safety

The management of the risks relating to workplace health and safety concerns any type of activity aimed at developing and putting in place a system for the prevention of and protection against workplace risks, in accordance with the contents of Legislative Decree No. 81/2008 (hereinafter, the Consolidated Law).

First of all, it should be recalled that, under the Consolidated Law, the employer is responsible for defining the company's policy on the health and safety of workers in the workplace.

In accordance with the provisions of such Law, the Company has adopted and keeps updated a “Risk Assessment Document” drawn up in accordance with national and European guidelines (INAIL, UNI-EN-ISO, European Agency for Health and Safety), containing:

- assessment of the health and safety risks to which workers are exposed in the course of their work activity;
- identification of the prevention and protection measures adopted to safeguard the workers and of the programme of measures deemed appropriate to upgrade safety levels within the short term;
- identification of the procedures for implementing the measures so identified, and of the corporate structures and officers responsible for them, who shall be solely persons possessing the appropriate competences and powers;
- identification of the officer responsible for the prevention and protection service, of the workers’ safety representatives and of the competent medical doctors who have participated in the risk assessment;
- identification of the tasks which might expose workers to specific risks requiring proven professional skills, specific experience and appropriate training and updating.

The company's "Occupational Health and Safety Management System" complies with current laws and is based on the most advanced standards in the field: UNI ISO 45001 (in 2018, ISO replaced the British Standard Occupational Health and Safety Assessment Series – OHSAS 18001:2007). The methods and operational processes by which the organisation meets the requirements of the aforementioned International Standard and guarantees the fulfilment of the provisions of Article 30 – Organisation and Management Models – of the Consolidated Law are set out in the corporate rules and in the Risk Assessment Document.

The company has adopted a system of functions appropriate to the nature and size of the organisation and type of activity carried out, ensuring the necessary technical competences and powers for risk verification, assessment, management and control. In addition, the processes managed by the Prevention and Protection and Occupational Medicine

department of the Intesa Sanpaolo Parent Company, which the company uses, are quality certified according to UNI EN ISO 9001: 2015.

The corporate Structures in charge of managing OH&S documentation, including authorisations/certifications/favourable opinions issued by the Public Administration, must comply with the rules of conduct set out and described in the protocol "*Management of activities relating to the request for authorisation or fulfilment of requirements towards the Public Administration*".

The company's occupational health and safety policy must be disseminated, understood, applied and updated at all organisational levels. The Company's general guidelines must target ongoing improvement of the quality of health and must contribute to the development of an effective "prevention and protection system". All the Company's structures must comply with the provisions on workplace health, safety and hygiene, and take them into due account whenever changes to the existing organisational setup are introduced, including workplace restorations/setups.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

Process description

The occupational health and safety risk management process, for which Neva relies on the support of the competent Parent Company structure on the basis of a service contract, consists of the following steps:

- identifying and classifying hazards (including both safety hazards and occupational health hazards);
- carrying out risk assessment;
- defining and developing prevention and protection measures;
- preparing an action plan and allocating actions among the various corporate structures;
- implementing the planned actions in the framework of a programme;
- monitoring implementation and checking the effectiveness of the measures adopted.

With specific reference to construction site management (Articles 88 et seq. of the Consolidated Law) which falls under the responsibility of the "Principal", the process comprises the following phases:

- verifying the technical and professional competence of the contractors/subcontractors and self-employed workers;
- appointment of the Project manager and, where necessary, of the Site engineer, the design Coordinator and the works Coordinator, subject to verification of the professional

requirements of the subjects in charge and formalisation in writing of the relevant appointments;

- planning of the works phases and their evaluation with special reference to the interactions of the activities also having an impact on the surroundings of the work site and the possible concurrence of the Company's activities and preparation of the safety and coordination plans or, where interference risk evaluation documents are not provided for by regulations, also on behalf of appointed professionals;
- preparation of requests for proposals with information to the counterpart as to the arrangements in place on the subject of health and safety (safety and coordination plans/interference risk evaluation documents);
- preparation of the proposal by the offeror with indication of the costs allocated to health and safety relating to the measures in place to manage interferences, on the basis of the scope and characteristics of the service/supply being offered, as well as containing a statement of acknowledgement of the risks present in the places where the work is carried out and of the relevant measures aimed at their elimination/reduction;
- fulfilment of technical-administrative obligations, notifications and communications to the public administration, including on behalf of the professionals in charge;
- awarding of the service and stipulation of the agreement, with the indication of the costs relating to safety and attachment of the safety and coordination plan/interference risk evaluation document;
- coordinating performance of activities by the various contractors/self-employed workers and carrying out site controls in compliance with the required measures, also through the professionals appointed for this purpose.

At temporary or mobile construction sites where Company employees are present, the risks arising from interference between the two activities are managed by the Principal, even through professionals specifically appointed for this purpose, by identifying the prevention, protection and emergency measures safeguarding the health and safety of the employees, customers, contractors and self-employed workers. Such measures are set out in the Safety and Coordination Plan or, if not provided for therein, in the Single Interference Risk Assessment Document (having regard to their respective scopes) prepared by the persons appointed by the Principal, with support, as required, of the Corporate Protection Function of the Parent Company.

With specific reference to the management of supply contracts, works contracts and service contracts (falling within the scope of Article 26 of the Consolidated Law) the process comprises the following phases:

- verifying the technical and professional competence of the contractors/subcontractors and of the self-employed workers;
- providing information to the subcontractors/self-employed workers on the specific risks at work sites, and on the prevention and emergency measures adopted, having regard to the activities covered by the contract; moreover, where provided for by the law or regulations, preparing the Interference Risk Assessment Document (DUVRI), to be supplied to bidders for the purpose of preparing their bid, and which will constitute an integral part of the contract, containing the appropriate measures for eliminating or reducing the risks arising from the interference of other activities with those required for contract performance, and simultaneous preparation of the request for bids, where provided for;
- preparation of the bid by the bidder, indicating any additional costs earmarked for safety measures and interference management measures, which shall be proportionate to the scope and characteristics of the supply/works offered, and shall contain a statement to the effect that the bidder has been informed of the risks present at the proposed construction site, together with a description of the proposed measures to eliminate/reduce those risks;
- award and signing of contract, indicating the cost earmarked for safety measures and annexing the DUVRI;
- performance of the supply/works contract by the selected contractor, cooperation and coordination with the subcontractors/self-employed workers to implement occupational risk protection and prevention actions, also via the exchange of information to eliminate the risks due to any interference between the works of the different contractors involved in performance of the overall project and the risks linked to the concurrent presence of the Company's agents, employees and customers on site;
- control on compliance with contractual requirements in performance of activities.

Even for the obligations set forth in the above mentioned Article 26, a delegation and sub-delegation system entered into force involving the corporate figures close to the risk sources, who can assess their impacts and set up the most appropriate measure to prevent them.

Procedures to manage and control the process are based on a clear, formalised assignment of duties and responsibilities with reference to the Structures involved (including external outsourcers) in controls on compliance with health and safety regulations in force from time to time, and on a consistent system of authority, that governs the functions and powers arising from the regulatory obligations of the Consolidated Law.

The operating procedures for managing the process and identifying the structures/roles in charge of the different phases are governed by internal rules, which are developed and updated by the competent Structures and form an integral and substantive part of this protocol.

In order to manage organisational complexity, the Bank has identified the business functions of the outsourcer Intesa Sanpaolo that are able to ensure a careful and effective management of occupational health and safety issues.

The Parent Company, the Company's outsourcer, has a single centre of specialisation and competence for health and safety issues. The Head of this structure is the Employer's Delegate, who is responsible for defining the guidelines, coordination and control and who is assigned all responsibilities in this area (except for the fulfilments governed by Title IV of Legislative Decree No. 81/08), including the power to identify in turn other corporate figures to whom tasks and responsibilities related to the roles held may be assigned, as well as, for the delegated functions, autonomy of expenditure and management, with provision for specific flows to the delegating party, as focal point and central contact person.

Control principles

The control system for monitoring the process described above must be based on the following elements:

- Authorisation levels defined within the process:
  - the company’s management system defines specific responsibilities and procedures to allow the full implementation of the workplace health and safety policy with a systematic and planned approach. In particular, the company figure that plays the role of "Employer" has been identified. This figure may issue instructions on the subject to the corporate Structures, enjoys the widest organisational autonomy and has the broadest spending powers, also with the power to delegate and sub-delegate pursuant to Article 16, paragraph 3 bis of the Consolidated Law;
  - a system of different functions is in place, to ensure the necessary technical competences and powers for risk verification, assessment, management and control;
  - all the persons/corporate roles taking part in the phases of the above-mentioned process must be identified and authorised by means of function delegation, to be issued and kept on file by the Employer, or by the authorised persons.
- Segregation of the duties between the different persons/corporate roles involved in the Risk Management Process relating to workplace health and safety. Specifically:
  - the operational Structures responsible for implementing and managing projects (real estate, IT, physical security, or relating to work processes and staff management),

shall be distinct and separate from the Structure which is appointed under the law and/or the internal rules, to provide advice on risk assessment and on the monitoring of risk prevention and reduction measures;

- the competent structures shall appoint persons having specific responsibilities for managing/preventing occupational health and safety risks;
- the Workers' Safety Representative actively cooperates with the Employer or their delegate in order to point out any critical issues and identify consequent solutions.

- Control activities:
  - the competent structures must activate a systematic company control plan in order to verify the correct application/management of the procedures and measures put in place to assess, in compliance with legal requirements, occupational risks. In particular, the plan shall cover:
    - corporate areas and activities to be assessed (of an organisational nature[66], health surveillance, worker information and training, and monitoring of workers' compliance with health and safety requirements in performance of their duties);
    - procedures for performing verifications, reporting procedures;

    The company plan must also ensure:
    - compliance with the technical-structural standards required by law in respect of equipment, plant, workplaces, and chemical, physical and biological hazards;
    - verification and, if these are not available on institutional sites, acquisition by the competent structures of the documentation and certifications required by law (concerning buildings, systems, persons, and companies, etc.);
    - compliance with the process and technical and administrative requirements set out in the internal regulations and applicable laws.

    An appropriate control system shall also be put in place with regard to the effective implementation and ongoing maintenance of the conditions of appropriateness of the measures adopted. The plan shall be reviewed and amended in an appropriate manner whenever significant infringements are detected to the rules on accident prevention and workplace hygiene or whenever organisational and operational changes are made to incorporate scientific and technological developments.
  - the competent structures shall ensure that all the planned prevention and protection measures are implemented, providing ongoing monitoring of risk situations and of the progress of the action plans established by the specific risk assessment documents. These Structures avail themselves, where necessary, of the

[66] Including emergencies, first aid, supply/works contract management, regular safety meetings, consultations with the workers' safety representatives.

collaboration of the Structures in charge of human resources management, procurement, training as well as the Structures for the management and implementation of building works, design and management of work processes, physical security, information systems, management and maintenance;

- the Workers' Safety Representative, acting in compliance with applicable legislation, is entitled to access the company's documents relating to risk assessment and associated prevention measures and to request additional information on the subject. The Representative shall also be authorised to access workplaces and make observations at the time of inspections and checks by the competent Authorities;
- all workplaces shall be visited and assessed by persons meeting the legal requirements and having appropriate technical qualifications. The Competent Doctor and the Head of the Prevention and Protection Service shall visit the workplaces where workers are exposed to specific risks and shall carry out spot checks in the other workplaces;
- specialist figures possessing proven professional expertise and meeting the requirements provided for by specific standards assessed on a prior basis, shall contribute to the assessment process and to planning protection measures in respect of specific risks, specifically:
  - the Competent Coordinator Doctor: appointed by the Employer or his/her representative, guarantees health surveillance obligations of regulations, assists the Employer and the Safety Department in assessing risks, preparing and adopting measures to protect workers' health and mental well-being; combines and updates, after notifying the Local Competent Doctors, the health surveillance protocols with related documentation and procedures;
  - The Local Competent Doctor: appointed by the Employer or his/her representative, for areas in its remit, plans and conducts health surveillance based on the health protocols defined considering specific risks using the general guidelines provided by the Competent Coordinator Doctor and the Risk Assessment Document, and gives an opinion on fitness for the specific task, notifying the outcome in writing to the Employer and worker;
  - the Person in Charge of Asbestos Risk: is appointed based on point 4 of Italian Ministerial Decree 06/09/94 and is "tasked with controlling and coordinating all maintenance activities that may involve materials in asbestos". In this respect, it coordinates maintenance activities concerning ACMs and supports the Employer in keeping appropriate documentation on the location of ACMs; in

ensuring compliance with safety measures (for cleaning activities, maintenance interventions and any event that may cause a disturbance of ACMs); in providing the building occupants with correct information on the presence of asbestos, on potential risks and on the behaviour to adopt;

- the Radiation Protection Expert: is appointed by the Employer or his/her representative, and conducts analyses and necessary assessments for the purposes of the physical surveillance of the protection of individuals of the population;
- the Expert qualified to manage radon clean-up activities: provides technical indications in order to adopt corrective measures to reduce the concentration of radon in buildings pursuant to Article 15 of Legislative Decree No. 101/10;
- the fire-fighting Professional: prepares preventive opinions, applications for the assessment of projects, certifications and statements on construction elements, products, materials, equipment, devices and plants which are relevant for fire safety purposes;

and as regards work sites (Title IV of the Consolidated Law):

- the Project Manager: is appointed by the Principal to carry out the duties assigned under Article 90. He/she takes on all powers and responsibilities of legal obligations to supervise the work site, also guaranteeing compliance with all safety regulations in applicable provisions;
- the Planning Coordinator: is appointed by the Principal or Manager in cases required by law. He/she is in charge of drafting the Security and Coordination Plan (PSC);
- the Works Coordinator: is required to carry out coordination at the work site and also control work procedures. The duties of the Works Coordinator include, among others, the “validation” of the operational safety plan, controls, with appropriate coordination and control actions, of companies performing works, independent workers, complying with the provisions applicable to them in the PSC and the correct adoption of work procedures. This Coordinator also suspends works in the event of a serious, imminent danger.

- the competent Structures identified by the Employer/Principal shall also assess the technical and professional competence of contractors or self-employed workers in respect of the tasks assigned to them;
- the competent Structures identified by the Principal shall assess the technical and professional competence of the Project supervisors, the Site engineer, and the

works Coordinator in relation to the specific characteristics of the works to be executed under the works contracts;

- if the documentation required under the Consolidated Law is maintained on electronic medium, the competent Structure shall check that the data saving methods and the procedures for accessing the data management system are in compliance with Article 53 of the Consolidated Law;
- the Employer and the principal, also through their delegated persons, each within their respective spheres of competence, acting in accordance with paragraph 3-bis of Article 18 of the Consolidated Law, shall supervise the compliance of agents, workers, competent doctors, designers, manufacturers, suppliers, and installers with their obligations under health and safety legislation through the above-mentioned company-wide systematic control plan.
- with regard to temporary or mobile worksites, the Principal verifies that tasks are correctly assigned and that the Site engineer, the Project manager, the design Coordinator and the works Coordinator, where appointed; for this purpose, the Principal receives from them periodic reports on the activities carried out, critical issues, if any, and the measures adopted to rectify them;
  - that the real estate and/or movable property to purchase to assign through finance leases are in conditions that ensure they conform to applicable regulations, checking that required conformity statements and documentation required by law have been provided;
  - that in cases of the repossession of real estate and/or moveable property, or where information is obtained concerning possible user violations of health and safety regulations even during the regular amortisation of the leasing contract, all related actions, also of a legal nature, functional to managing occupational health and safety risks, are carried out diligently and in adequate times;
  - that the repossessed real estate and/or moveable property have been assessed for exposure to occupational health and safety risks, and actions to make them safe have been planned;
- the competent Structures identified by the Employer, check that the qualifications and requirements of the Competent Doctors and specialists that are involved in individual processes are maintained over time;
- the Officer notifies the competent Structures identified by the Employer of any delay in complying with the provisions of the Competent Doctor, in order to activate necessary measures;

- the competent Structures identified by the Employer, periodically check the correct management of preliminary investigations into occupational accidents.

- Process traceability including both the electronic and the paper trail:
  - in order to allow reconstruction of responsibilities, each Structure of the Company or of the outsourcer from time to time concerned shall put in place adequate systems for recording activities performed, and shall be responsible for filing and storing, also in telematic or electronic format, all executed contracts and all the documentation produced as part of its activities relating to management of workplace health and safety risks and the associated control activity;
  - the use of systems for the electronic management of data and documentation required by the Consolidated Law must comply with Article 53 of the same;
  - each Structure from time to time concerned shall be responsible for acquiring, storing and filing the documents and certifications required by law, if these are not available on institutional sites, as well as any documentary evidence of the technical and professional expertise of contractors, self-employed workers and persons appointed as responsible for workplace safety (e.g. the Project manager, design and works Coordinators);
  - management of the different risk contexts provides for the use of specific information systems accessible via the intranet by all the Structures concerned and authorised to carry out risk assessments relating to the operating units. These information systems shall contain, for example, the technical documentation of plant, machinery, workplaces, etc., the lists of employees exposed to specific risks, the health documents (in compliance with the confidentiality requirements provided for by legislation), training and information activities, risk elimination/reduction activity, internal and external inspections, information on injuries and risk reporting, forms for the management of environmental monitoring and health records, etc..

Rules of conduct

The Company and outsourcer Structures howsoever involved in the management of the risks relating to workplace health and safety, as well as all employees shall comply with the procedures set out in this protocol, the applicable provisions of law, internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular, all the Structures/roles are obligated – within their respective spheres of competence – to:

- ensure, within their sphere of competence, performance of the measures relating to occupational health and safety, by implementing general protection measures and assessing the choice of work equipment and workplace layout and organisation;

- if third parties are to be involved in the management/prevention of workplace health and safety risks, the contracts entered into with such persons shall contain a specific declaration that they are aware of the provisions of Legislative Decree No. 231/2001 and undertake to comply with them;
- avoid appointments of external consultants that are not made on substantiated and objective grounds of qualified professionalism and expertise, competitiveness, price, integrity and the ability to provide effective assistance. In particular, the rules for the selection of professionals shall refer to the criteria of clarity and availability laid down in the Group's Code of Ethics and Internal Code of Conduct;
- adopt transparent and cooperative conduct towards the Agencies in charge of performing controls (e.g. Labour Inspectorate, Local Health Authorities, the Fire-fighting agencies, etc.) when such agencies carry out checks or inspections;
- when awarding supply and works contracts, inform the contractors of the specific risks present at the worksites where they will operate, and apply measures to ensure the safe management of any interferences between contractors, including any self-employed workers, highlighting the planned cost of safety measures in the contracts where such indication is provided for;
- foster and promote internal information and training on work-related risks, on the prevention and protection measures and activities adopted, first aid procedures, fire-fighting measures and evacuation plan;
- ensure compliance with the health and safety rules and legislation by all workers who are not Company employees, with particular reference to the contracts governed by Legislative Decree No. 276/2003 as subsequently amended and supplemented, to individuals operating under training schemes and to any third parties who might be present in the workplaces;
- ensure that, in respect of automatic data processing systems, data saving methods and the procedures for accessing the required documentation management system meet the requirements set out in Article 53 of the Consolidated Law.

Likewise all employees shall:

- comply with legal provisions and internal regulations and directives given by the company's Structures and the competent Authorities;
- use in an appropriate manner machinery, equipment, tools, means of transport and all other work equipment, and safety devices;
- report immediately to the officer in charge of emergencies or his subordinates any potential or real danger situation and, in case of emergencies, take all steps within their competences and possibilities, to eliminate or reduce the hazardous situation.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offences covered by Legislative Decree No. 231/2001.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.8 Sensitive area concerning computer crime

7.8.1 Type of offence

Law No. 48 of 18.3.2008 ratified the Convention on Cybercrime of the Council of Europe, signed in Budapest on 23.11.2001, aimed at fostering international cooperation between the States parties to the Convention in order to combat the spread of cybercrime directed against the confidentiality, integrity and availability of computer systems, network and data, especially in consideration of the nature of such crimes, whose planning or commission often involve different countries.

The reform of the legislation on cybercrime was carried out both by introducing new types of crimes in the Criminal Code and by amending certain existing crimes. Article 7 of the Law has also added to Legislative Decree No. 231/2001 Article 24-bis, which lists the series of computer crimes which might give rise to the administrative liability of Entities.

The above-mentioned law has also amended the Code of Criminal Procedure and the provisions relating to the protection of personal data, essentially in order to facilitate investigations of computer data and allow for the preservation of internet traffic data for certain periods. On the other hand, the Italian legal system has not implemented the definitions of "computer system" and "computer data" provided by the Budapest Convention; such definitions, which are reproduced hereunder, may however be taken as a reference by case law in this area:

- "computer system" means: any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- "computer data" means: any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

The predicate offences listed by Article 24-bis of Legislative Decree No. 231/2001 are described below.

Unauthorised access to a computer or telecommunications system (Article 615-ter of the Criminal Code)

The offence is committed by anyone who unlawfully enters or remains in a computer or telecommunications system protected by security measures against the express or tacit will of the person entitled to exclude them.

For the offence to occur it is not necessary that it be committed for the purpose of making a profit or damaging the system; the offence occurs also where the purpose is to demonstrate the hacker's ability and the vulnerability of the system; however, unauthorised access is in

most cases aimed at damaging the system or perpetrating frauds or committing other computer crimes.

The offence is prosecutable on the action of the injured party; however, it is prosecutable ex officio where the specific aggravating circumstances set out in the Article are present, including: if the deed causes the destruction or the damage of the data, the software or the system or the partial or total interruption of its operation; if the deed concerns systems of public interest; or if the deed was committed by abusing one's role as system operator.

In the corporate context, the offence may also be committed by any employee who, while possessing system access credentials, accesses parts of the system which are off limits to him, or accesses, without authorisation a database of the Company (or also of third parties which the Company is licensed to use), by using the credentials of other, authorised, co-workers.

Unauthorised possession or dissemination of access codes to computer or telecommunications systems (Article 615-quater of the Criminal Code)

Distribution of computer equipment, devices or programs intended to damage or interrupt a computer or telecommunications system (Article 615-quinquies of the Criminal Code)

Article 615-quater punishes any person who, in order to procure a profit for themselves or others or to cause damage to others, unlawfully obtains, reproduces, disseminates, communicates or delivers codes, passwords or other means of access to a system protected by security measures or in any case provides suitable indications for that purpose.

Article 615-quinquies punishes any person who procures, produces, reproduces, imports, disseminates, communicates, delivers or makes available to others equipment, devices or programmes for the purpose of unlawfully damaging a system or the data and programmes pertaining thereto or of facilitating the interruption or alteration of its operation.

These offences, which are punishable ex officio, also occur in the event of unauthorised possession or dissemination of passwords or of potentially damaging programmes (virus, spyware) or devices regardless of whether the other computer crimes illustrated above – which might be prepared by these actions – are actually committed or not.

One condition for the first offence is the intention of obtaining profit or causing damage. However, for the purpose of assessing such types of conduct, one key element might be the objectively abusive nature of the transmission of data, software, email, etc., by persons who, while not intending to obtain profit or causing damage, are aware of the presence in

such data etc. of a virus which might cause the harmful occurrences described in the provision.

Wiretapping, blocking or illegally interrupting computer or information technology communications (Article 617-quater of the Criminal Code)

Installation of equipment designed to wiretap, prevent or interrupt computer or telematic communications (Article 617-quinquies of the Criminal Code).

The conduct punished by Article 617-quater of the Criminal Code consists in fraudulently wiretapping communications within a computer system or telecommunication system or between several systems, or blocking or interrupting such communications. The same offence is committed, unless the deed constitutes a more serious offence, when the contents of the above-mentioned communications are disclosed to the public by any means of communication.

Wiretapping can be performed either by technical devices or through the use of software (spyware). The blocking or interruption of communications ("Denial of service") may also consist of slowing down communications and can be achieved not only by using computer viruses, but also for example by causing system overload by generating a vast number of fake communications.

The offence is prosecutable on the action of the injured party; however, it is prosecutable ex officio where specific aggravating circumstances set out in the Article are met, including where the offence is committed against a computer or telecommunication system used by the State or by another public Entity or used by a company that provides public services or services of public interest, or where the offence is committed by abusing the role of system operator.

Within the company, the blocking or interruption of communications may for example be caused by the unauthorised installation of a software system by an employee.

Article 617-quinquies applies when a person, outside the cases permitted by law, installs equipment designed to wiretap, prevent or interrupt communications relating to a computer or telecommunications system or between several systems, irrespective of the occurrence of such events. This offence is prosecutable ex officio.

Damaging computer information, data and programs (Article 635-bis of the Criminal Code)

Damaging computer information, data and programs used by the Government or any other public body or by an entity providing public services (Article 635-ter of the Criminal Code)

Article 635-bis of the Criminal Code punishes, unless the deed constitutes a more serious offence, any person who destroys, damages, deletes, alters or suppresses computer information, data or software belonging to others.

According to a strict interpretation, the concept of "software belonging to others" might also include software used by the person under a licence granted by the lawful owners of the software.

Article 635-ter of the Criminal Code, unless the fact constitutes a more serious offence, punishes any conduct aimed at producing the occurrences described in the preceding Article, regardless of whether material damage actually occurs: any such material damage constitutes an aggravating circumstance. This offence applies only to conduct aimed at damaging computer information, data or software used by the Government or another public Entity or by an organisation providing a public service. Therefore, this type of offence also includes conduct aimed at damaging data, information and software used by private organisations, where they are intended to provide public interest services.

Aggravating circumstances for both offences exist where the deed is committed with violence to individuals or threat, or by abusing the role of system operator. The first offence is prosecutable on the action of the injured party, or ex officio where one of the aggravating circumstances occurs; the second offence is always prosecutable ex officio.

If the conducts described are committed through unauthorised system access, they shall be punished under the above-mentioned Article 615-ter of the Criminal Code.

Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)

Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

Article 635-quater of the Criminal Code, unless the fact constitutes a more serious offence, punishes any person who, by the conducts referred to in Article 635-bis, i.e. by introducing or transmitting data, information or software, destroys, damages or makes it impossible, either in whole or in part, to use another person's computer or telecommunication system or seriously obstructs its functioning. For this offence to be committed, the system so attacked must be damaged or rendered unusable at least in part, or its functioning must be obstructed.

Article 635-quinquies of the Criminal Code punishes the same conduct set out in Article 635-quater even where no actual damage occurs. Where damage does in fact occur, this constitutes an aggravating circumstance (it should however be noted that the material obstruction to the system's functioning is not expressly included among the aggravating

circumstances). For this Article to apply, the computer or telecommunications systems so attacked must be of public interest.

This provision, differently from Article 635-ter, contains no reference to use by Public Bodies: it would seem therefore that for this offence to occur, the systems attacked must simply be “of public interest”; therefore, on the one hand, their use by Public Bodies would not suffice, and on the other, the rule would also be applicable to systems used by private organisations acting for public interest purposes.

Both offences are prosecutable ex officio; aggravating circumstances occur where the deed is committed with violence to individuals or threat, or by abusing the role of system operator.

It would seem that the offence of system damage subsumes data and software damage where the latter have the effect of making the systems unusable or of severely obstructing their regular functioning.

If the conducts described are committed through unauthorised system access, they shall be punished under the above-mentioned Article 615-ter of the Criminal Code.

Forgery of electronic documents (Article 491-bis of the Criminal Code)

Article 491-bis of the Criminal Code applies to public or private computer documents having probative value the same treatment applicable to forgery of traditional paper documents, as set out in Articles from 476 to 493 of the Criminal Code. They include in particular material falsification or provision of intentionally false statements committed by a Public Official or by a private individual, falsification of registers and notifications, intentionally false statements in certificates by providers of public interest services, and the use of a false act.

In current legislation, the concept of electronic document is independent of the material medium containing it, since the element having relevance in criminal law for the purpose of identifying the electronic document is whether such document can have probative value according to the rules of civil law[67].

In the offences of false deeds/forged deeds, one fundamental distinction must be made between material falsity and an intentionally false statement (falso ideologico): material falsity means the real author of the document is not the stated author, or that the document

[67] On this point it should be noted that under the Digital Administration Code (Article 1, point p) of Legislative Decree No. 82/2005), an electronic document is “the electronic representation of acts, facts or data having legal significance”, but:

- if such document is not signed with an electronic signature (Article 1, point q), it cannot have probative value, but can at the most, at the Court’s discretion, satisfy the legal requirement of the written form (Article 20, paragraph 1-bis);
- where the document is signed with "simple” (i.e. unqualified) electronic signature it cannot have probative value (and for the purpose of assigning probative value the Court shall assess the objective characteristics of quality, security, integrity and inalterability of the electronic document);
- an electronic document signed with digital signature or any other kind of qualified electronic signature shall have the probative weight of a private deed as laid down in Article 2702 of the Civil Code unless a claim of falsity is made, if the signature is recognised by the person against whom the document is asserted.

was altered (also by its original author) after being produced; an intentionally false statement occurs when the document contains untrue or unfaithfully reported statements.

As concerns computer documents having probative value, material falsity may occur where some other person's electronic signature is used, whereas alteration of the document subsequent to its preparation seems unlikely.

On the other hand, the provisions that punish the signing of blank sheets of paper (Articles 486, 487, 488 of the Criminal Code) do not seem to be applicable to electronic documents.

The offence of use of false acts (Article 489 of the Criminal Code) punishes any person who, while not taking part in the falsification of an act, uses such false act despite being aware of its falsity.

Computer crime by the certifier of a digital signature (Article 640-quinquies of the Criminal Code)

This offence is committed by a person responsible for certifying electronic signatures and who, in order to gain an unjust profit for himself or for others or to cause damage to others, infringes the legal obligations concerning issuance of a qualified certificate[68].

The author of the offence can obviously only be a "certification service provider" who performs specific certification functions in respect of qualified electronic signatures.

In this specific regard, it is noted that the company does not have the status of a "certification service provider"

Obstructing procedures to define, manage and control the "National cyber security perimeter" (Article 1, paragraph 11, Law Decree 105/2019)

The crime punishes anyone who, in order to obstruct or influence the Authorities in charge of protecting the strategic technological infrastructure system:

1) provides information, data or factual elements not corresponding to the truth, which are significant:
   a) for preparing and updating lists of networks, systems (including the relative architecture and components) and IT services of the PA and of public and private operators based in Italy, on whom the operation of an essential State function or provision of an essential service for fundamental civil, social or economic activities depends, and of which the malfunction, interruption or misuse may harm national security;
   b) for the communications that the aforesaid public and private operations must provide to the CVCN (National Evaluation and Certification Centre, set up by the Ministry for

[68] Under Article 1 points e) and f) of Legislative Decree No. 82/2005, qualified certificate means an electronic attestation which links a signature verification device to a person, confirms the identity of that person and meets the requirements laid down in Annex I to Directive 1999/93/EC and is provided by a certification service provider – i.e. a person providing electronic signature certification services or similar electronic signature related services – who fulfils the requirements laid down in Annex II to the same Directive.

Economic Development) of the supply contracts they intend stipulating to procure ICT assets, systems and services intended to be used with the aforesaid networks, systems and services;

c) for carrying out audit and supervisory activities concerning compliance with provisions and procedures for the preparation and updating of the above lists, the notification of supplies and incidents and the security measures relative to the aforesaid systems, networks and services;

2) omits notifying the aforesaid data, information or factual elements within the times indicated.

More generally, it should be noted that some types of computer crimes in concrete terms might well not fulfil the requirement of being committed in the Company's interest or for its benefit, which must be present for the Company to incur administrative liability. However, where all the elements provided for by Legislative Decree No. 231/2001 occur, the Company may be held liable, in accordance with the provisions of Article 8 of the Decree, even where the author of the offence cannot be identified (in this case, the offender, albeit unidentified, should at least be proven to be a manager or an employee). This eventuality is certainly not unlikely in the field of computer crime, in the light of the complexity of the medium and of the evanescence of cyberspace, which also make it objectively difficult to identify the specific place where the offence may have been committed.

Lastly, it should be recalled that Article 640-ter of the Criminal Code, which punishes the crime of computer fraud perpetrated against the State or another Public Body, also constitutes a predicate offence of the administrative liability of Entities; in this respect, see Chapter 7.2.1.

7.8.2 Sensitive company activities

The Company's activities in which computer crimes can be committed and computerised corporate data unlawfully processed are specific to any business area that uses information technology.

The Company has put in place specific organisational safeguards and has adopted appropriate security solutions, in compliance with Supervisory Authority regulations and with the European and national regulations on data protection, to ensure prevention and control of risks relating to information technology (IT) and cyber security, to protect its information assets and customers and third parties.

The sensitive activity identified by the Model in which the risk of the unlawful conduct described above is greatest is "Management and use of IT systems and Information assets".

We reproduce below the protocol laying down the control principles and rules of conduct applicable to this activity, as well as the detailed corporate regulations governing this activity.

This protocol also applies to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.8.2.1 Management and use of IT systems and Information assets

This protocol applies to all the Company Structures involved in the management and use of computer systems and Information assets.

In particular, it applies to:

- all persons involved in the management and use of information systems that interconnect with/use software of the Public Administration or the Supervisory Authorities;
- all the Structures entrusted, also on the basis of specific outsourcing contracts, with the design, implementation or management of IT, technological or telecommunications tools;
- all the Structures responsible for implementing organisational, regulatory and technology actions to ensure the protection of the Group's Information assets in the activities falling under their competence and in relations with third parties with access to Information Assets;
- all the professional roles involved in company processes and operating therein for any reason, whether as employees or as collaborators or freelance professionals, who use the Company's information systems and process the data of the Information Assets.

Pursuant to Legislative Decree No. 231/2001, the relevant processes could present opportunities for the commission of computer crimes covered by Article 24-*bis*, as well as the offence of computer fraud to the detriment of the State or other public body covered by Article 640-*ter* of the Criminal Code and referred to in Article 24 of the Decree. Furthermore, access to the computer networks could also provide a means for committing offences against intellectual property rights.

These offences could be committed in order to gain access to data or information belonging to others or to destroy, deteriorate, delete, alter or suppress information, data or computer programs belonging to others for the benefit of the Company, as well as to make false reports through the disclosure to third parties of passwords or access codes to information systems of the Supervisory Authorities. Furthermore, access to the computer networks could also provide a means for committing offences against intellectual property rights[69].

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question.

[69] For a description of the relevant conduct see Chapter 7.8.

Process description

The use and management of computer systems and of Information Assets are essential activities for the performance of corporate business and characterise most of the Company's processes.

The information systems used by the Company also include hardware and software for the fulfilment of obligations towards the Public Administration or the Supervisory Authorities that require the use of specific programs provided by the same Bodies, or direct connection with them.

Hence the necessity to identify effective and stringent rules and measures relating to organisational, behavioural and technological security, and design specific control measures ensuring that the IT systems and the Group's Information Assets are operated and managed in full compliance with current legislation.

In this regard, it should be noted that the Company has entered into a specific outsourcing contract with Intesa Sanpaolo in the field of information systems that includes, among others, the management of IT security, as well as design, development, management and support in the IT field. Specific security measures consistent with the control principles of this Model are foreseen for applications made available to or used by third-party suppliers with respect to the Parent Company.

Below are the details of the relevant processes under this protocol managed through the outsourcing contract in place with Intesa Sanpaolo.

The computer security management process comprises the following phases:

- analysis of computer risk and identification of computer security requirements;
- management of Computer Resource Accesses and ICT Security Services;
- management of regulations and computer security architecture;
- monitoring IT security events and managing critical IT security events;
- third-party security (classification and monitoring of suppliers of the Company or Parent Company);
- fostering of an IT security culture;
- design and implementation of computer security solutions.

The fraud prevention process involves the following phases:

- identification of the appropriate measures to upgrade prevention;
- monitoring of developments in computer crimes, also with regard to related physical security aspects;
- management of the activities necessary to identify and resolve threats to company assets;

- management of communications with Law Enforcement Bodies.

The physical security management process comprises the following phases:

- managing the protection of areas and premises where the activity is performed;
- managing the physical security of peripheral systems (central headquarters, other sites).

The process relating to the electronic signature certification service comprises the following phases:

- opening the contract;
- registering the holder;
- managing the certificate (suspending, reactivating, revoking, renewal and PIN unlocking).

The process for the design, development and implementation of the ICT services comprises the following phases:

- design, implementation and management of the corporate software solutions and technology infrastructure.

The ICT management and support process comprises the following phases:

- provision of ICT services;
- monitoring of the operation of ICT services and management of any malfunctions;
- user assistance via Help desk and problem solving activities.

The process to manage communications to the Authorities in charge of defining, managing and controlling the "National cyber security perimeter" comprises the following phases, in compliance with expected Government implementing measures:

- the identification of information and events that must be notified/reported;
- the transmission, depending on the relevant Authorities, of the communication/reporting, by competent functions.

In view of the outsourcing of the activities in question to the Parent Company, the operating procedures for the management of the processes are governed by the relevant Intesa Sanpaolo regulations.

Control principles

Without prejudice to the security requirements of the Public Administration or Supervisory Authorities' software used by the Company, the control system protecting the processes indicated, in line with the internal policies on IT security, must be based on the following factors:

- Authorisation levels defined within each operating step of the process described above. Specifically:

- authorisations are managed by defining “access profiles” on the basis of the functions performed by each individual within the Company;
- changes to the content of the profiles are made by the relevant structures of the outsourcer, at the request of the Structures concerned. The requesting Structure must in any case ensure that computer authorisations required match the work duties of each individual;
- each user is associated with only one authorisation profile, on the basis of his role in the organisation and in compliance with the “least privilege” rule. In the event of user transfer or change of activity, a new authorisation profile will be defined, tailored to the newly assigned role;
- the installation, implementation and modification of software in the Company's workstations (fixed and portable workstations) and servers may only be carried out by persons with specific authorisations.

Periodically, the appointed structure carries out a review of the users and authorisation profiles assigned.

- Segregation of duties:
  - different roles and responsibilities are assigned in respect of information security management; in particular:
    - assigning specific responsibilities ensures control over the areas of security direction and governance and planning, implementation, operation and control of the countermeasures adopted to protect corporate Information Assets;
    - precise responsibilities for the management of security issues are assigned to the organisational functions responsible for developing and managing information systems;
    - responsibilities and mechanisms are defined to ensure the management of abnormal security events, emergency and crisis situations and communications to the relevant Authorities;
    - precise responsibilities for preparing, validating, issuing and updating the security rules are assigned to corporate functions different from those in charge of computer security management.
  - the activities of implementing and modifying software, managing computer procedures, physical and logical access controls and software security controls are organisationally assigned to structures which are different from the users, to ensure sound management and ongoing control over the information system management and use process;

- precise responsibilities are assigned to ensure that the software development and maintenance process, whether performed in-house or by third parties, is managed in a controlled and verifiable manner, following an appropriate authorisation process.

- Control activities: the management and use of the Company's information systems and of Information assets undergo ongoing control activity by using appropriate information protection measures, so as to safeguard its confidentiality, integrity and availability, with particular reference to the handling of personal data, and by adopting for the overall set of corporate processes specific operating continuity solutions of a technological, organisational and infrastructural nature, able to ensure continuity in the event of emergency situations. These control activities also provide valid support ensuring traceability of all changes made to computer procedures, the identification of the users who have made such changes and of those who have carried out controls on the changes made.

  The planned controls, set out in the relevant internal policies, shall be based on identification of specific activities targeting long-term management also of the aspects relating to protection of the Group's Information assets, such as:

  - defining security objectives and strategies;
  - defining a risk analysis method for the Information Assets, to be applied to the company's processes and assets, estimating the greatest risks the information is exposed to with regard to the criteria of confidentiality, integrity and availability;
  - identifying appropriate countermeasures against the risk levels detected, monitoring and checking that such security levels are properly maintained;
  - delivery of appropriate staff training on computer security aspects in order to raise their awareness of and alertness to the issue;
  - preparing and updating security rules, in order to ensure their sustained applicability, adequacy and effectiveness;
  - controls on correct application and compliance with the defined legislation.

  The main control activities performed from time to time, and set out in detail in the reference internal rules, are the following.

  With reference to physical security:

  - protection and control of physical areas (perimeters/reserved areas) to prevent unauthorised accesses to, or altering or theft of information assets.

  With reference to logical security:

  - identification and authentication of user identification codes;
  - authorising requests for access to information;

- provision of encryption and digital signature technologies to ensure the confidentiality, integrity and of stored of transmitted information and prevent its rejection.

With reference to the operation and management of applications, systems and networks:

- ensuring separation of the premises (development, testing and production) in which the systems and their applications are installed, managed and maintained, in order to ensure their sustained integrity and availability;
- preparing and protecting system documentation concerning configurations, customisation and operating procedures, to ensure the appropriate and secure performance of activities;
- putting in place of measures for software under development in terms of installation, management of operation and emergencies, and code protection, ensuring the preservation of the confidentiality, integrity and availability of the information handled;
- implementing actions to remove systems, applications and networks identified as obsolete;
- planning and managing the rescue of operating systems, software, data and system configurations;
- managing data storage devices and media to ensure their long-term integrity and availability by regulating and controlling use of the devices, equipment and all information assets assigned, and by defining procedures for the custody, re-use, reproduction, destruction and physical transport of removable data storage media in order to protect them from damage, theft or unauthorised access;
- monitoring applications and systems, by defining efficient criteria for the collection and analysis of the relevant data, in order to allow identification and prevention of non-compliant actions;
- prevention of malware by means of appropriate tools and infrastructure (including antivirus systems) and by assigning responsibilities and setting up procedures for the phases of installation, verification of new releases, updates and actions to be implemented when potentially damaging software is identified;
- formalising responsibilities, processes, tools and procedures for exchanging information by e-mail and through websites;
- adopting appropriate safeguards to achieve the security of telecommunications networks and supporting devices, and ensure the correct and safe circulation of information;

- establishing specific procedures covering the stages of system and network design, development and replacement, defining solution acceptance criteria;
- establishing specific procedures to ensure that any materials covered by intellectual property rights are handled in accordance with legal and contractual provisions;
- preparation and updating of specific technological and application inventories for the purposes of communication with the relevant Authorities.

With reference to application development and maintenance:

- identifying appropriate countermeasures and controls to protect the information handled by the applications, meeting the requirements of confidentiality, integrity and availability of the information handled, having regard to the areas and use procedures, integration with existing systems and compliance with the provisions of law and with internal rules;
- putting in place appropriate security controls throughout the application development process, to ensure their correct operation, including systems for restricting access to authorised persons only by means of tools, external to the application, for identification, authentication and authorisation.

With reference to the management of security failures:

- establishing appropriate reporting channels and procedures for promptly reporting incidents and suspicious situations, in order to minimise any consequent damage, prevent repetition of inappropriate conduct and initiate a response process which may also lead to declaration of a state of crisis.

With reference to the management of communications with the relevant Authorities:

- controls on the accuracy of communications with particular reference to the deadlines indicated for sending information, notifications and reporting incidents.

- Process traceability including both the electronic and the paper trail:
  - the decision-making process, with reference to the management and use of IT systems, is ensured by full system-wide traceability;
  - all occurrences and the activities carried out (including access to information, mitigation actions performed via the system, for example accounting adjustments, changes in user profiles etc.), with particular regard to the actions carried out by privileged users, are tracked through systematic recording (log file system);
  - all accesses to and exits from reserved areas by duly authorised staff who actually need to access such areas, shall be recorded by dedicated tracking mechanisms;
  - all operations performed on the data shall be tracked, compatibly with current laws, in order to allow reconstruction of the responsibilities and of reasons for the choices made; moreover, each Structure shall be responsible for filing and storing the

documentation it has produced, also in telematic or electronic format, which falls under its competence.

Rules of conduct

The Company's structures, howsoever involved in the activity of management and use of computer systems and of Information assets shall comply with the procedures set out in this protocol, the applicable provisions of the law, the internal rules and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

Specifically:

- all persons involved in the process must be duly appointed;
- employees or, in general, persons involved in the process are required to report to the Chief Executive Officer any security incidents (also concerning attacks on the computer system by external hackers), making available and archiving all the documentation relating to the incident and activating any escalation that may also lead to the opening of a state of crisis and communications to the competent Authorities;
- each employee is responsible for the correct use of the computer resources assigned to him (e.g. desktop or laptop personal computers), which are to be used solely for performance of his work duties. Such resources shall be kept with due care, and the Company must be informed without delay of any instances of theft or damage;
- where third parties/outsourcers are to be involved in the management of the Group's IT systems and Information assets and in the interconnection with/use of the software of the Public Administration or the Supervisory Authorities, the contracts entered into with such persons shall contain a specific declaration that they know the provisions of Legislative Decree No. 231/2001 and undertake to comply with them;
- the payment of fees or compensation to external collaborators or consultants involved is subject to permission given in advance by the organisational unit responsible for assessing service quality and the resulting fairness of the fee demanded; in any case, no remuneration shall be payable to employees or external consultants where not fully justifiable by the type of work performed or to be performed.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- enter without authorisation, either directly or through an intermediary, a computer or telecommunications system protected by security measures against the will of the holder of the right of access, including for the purpose of acquiring confidential information;

- access the Company's and the Group's computer system or telecommunications system or part thereof, or databases or parts thereof, without holding credentials or using the credentials of authorised colleagues;
- fraudulently wiretap and/or disclose to the public through any information system, communications within a computer system or telecommunication system or between several systems;
- use unauthorised technical devices or software tools (viruses, worms, trojans, spyware, diallers, keyloggers, rootkits, etc…) able to hinder or interrupt communications within a computer or telecommunications system or between several systems;
- introduce or transmit data, information or programmes to destroy, damage, make entirely or partially unusable, or prevent the functioning of information or computer systems of public utility;
- procure, reproduce, disseminate, communicate, or make available to others computer equipment, devices or software in order to illegally damage a system or the data and software contained therein or to assist the interruption or the altering of such system's operation;
- gain unauthorised access to a computer or telecommunications system of others, as well as seriously damaging or obstructing its operation;
- hold, procure, reproduce or disseminate access codes or other suitable means of access to a system protected by security measures without authorisation;
- destroy, damage, cancel, alter or suppress information, data or software programs owned by third parties or endanger the integrity and the availability of computer information, data or software used by the Government or another public body or relating to them or howsoever of public interest;
- alter electronic documents by using another person's electronic signature or by any other means;
- produce and transmit electronic documents containing false and/or altered data;
- carry out, through access to a computer network, unlawful conduct constituting breaches of intellectual property rights, including, for instance:
    - dissemination in any form of intellectual property not intended for publication or misappropriate their authorship;
    - copying, holding or disseminating in any form without being authorised computer programmes or audiovisual or literary works;
    - retaining any means intended to remove or circumvent the protective devices of processing programmes;

- reproducing databases on media not marked by the Italian Society of Authors and Publishers (SIAE), disseminating them in any form without the copyright holder's authorisation or in breach of the prohibition established by the maker;
- removing or altering digital information entered in protected works or appearing in disclosures to the public, concerning relative rights;
- importing, distributing, installing, selling, modifying or using devices for unscrambling restricted access audiovisual transmissions, also where these are receivable free of charge.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

7.9 Sensitive area concerning crimes against industry and trade and crimes involving breach of copyright and customs' law

7.9.1 Type of offence

Law No. 99 of 23/7/2009 – Provisions for the development and internationalisation of enterprises, and measures on energy – under a broad framework of initiatives to re-vitalise the economy and protect the authenticity of the "Made in Italy" label, and safeguard the interests of consumers and competition, has included a number of offences within the sphere of the liability of Entities, including certain offences introduced or reformulated by the same law. In particular, in the amended version of Legislative Decree No. 231/2001, Articles 25-bis and 25-bis.1 refer to offences set out in the Criminal Code relating to industry and trade[70], while Article 25-novies in order to strengthen the fight against intellectual property piracy[71] and counter the serious economic damage it causes to authors and to the related industry – refers to offences set out in the copyright law (Law No. 633/1941).

Smuggling crimes are included in the aforementioned provisions, introduced in Article 25-sexiesdecies[72] in order to implement the provisions of European legislation aimed at protecting the interests of the public finance of the European Union.

The offences in question are described below.

Counterfeiting, alteration or use of distinctive marks of intellectual works or industrial products (Article 473 of the Criminal Code)

The offence is committed by any person who, despite being able to ascertain that trademarks and other distinctive marks of industrial products belong to other parties, counterfeits them, or alters the original marks, or uses counterfeit marks without having taken part in their counterfeiting[73].

Counterfeiting occurs where a mark is reproduced faithfully or its essential elements are imitated so as to appear authentic on initial perception. These are classified as material falsifications likely to harm public reliance on the fact that the products or services so

[70] Subsequent to the amendment introduced by Law No. 99/2009, Article 25-bis of Legislative Decree No. 231/2001 – which formerly only concerned counterfeiting of money and official stamps – has been extended to cover the crimes set out in Articles 473 and 474 of the Criminal Code, which share with the former the legal asset which is mainly protected, i.e. the public trust, seen as the confidence that the public places in the genuineness of specific objects, marks or logos.

[71] Pursuant to Article 1 of Law No. 633/1941, intellectual works protected by copyright are those belonging to literature (including scientific and educational literature), music, the figurative arts, architecture, theatre, and film, irrespective of their form of expression. Computer software and data banks which by their choice of arrangement of materials constitute an intellectual creation of their author are also ranked as literary works.

[72] See Article 5 of Legislative Decree No. 75/2020

[73] The term "use" of the counterfeit marks means ancillary types of conduct, such as, for instance, placing on one's products counterfeit marks which have been falsified by third parties. In other words, it concerns types of conduct different from either putting into circulation products bearing counterfeit marks, covered by Article 474 of the Criminal Code, or from those conducts specifically related to counterfeiting, such as reproducing another party's mark in one's advertising, in commercial correspondence, in websites etc.

marked come from the company which is the holder, licensee or concessionaire of the registered mark. According to case law marks still unregistered are also protected, where an application has already been filed, since such application makes it formally knowable. For this conduct to constitute an offence, it must be engaged in intentionally; intention may also exist where the author of the conduct, while not having the certainty that the mark has been registered (or that an application for registration has been filed), fails to implement the appropriate checks despite having reason to harbour such doubt.

The second paragraph punishes the conduct of counterfeiting, as well as the use, by another party who did not take part in the counterfeiting of patents, designs and industrial models belonging to others[74]. This Article too aims at combating material counterfeiting which, in this type of offence, concerns documents proving the granting of the patents or model registrations. On the other hand, violation of the rights of exclusive economic exploitation of a patent is punishable under Article 517-ter of the Criminal Code.

Introducing into the country and selling products bearing counterfeit marks (Article 474 of the Criminal Code)

Article 474 of the Criminal Code punishes the conduct of those who, not having committed the offences covered by Article 473 of the Criminal Code, introduce into the territory of Italy industrial products bearing counterfeit or altered marks or distinctive signs, or hold for sale, sell or howsoever put into circulation counterfeit products, if they are not already punishable for having introduced them into the territory of Italy. To give rise to this offence, the conduct must be aimed at gaining a profit.

The holder of such products may be punishable, in addition to the offence in question, also for receipt of stolen goods, if at the time of purchasing the products he was aware of the falsity of the distinctive signs placed on the product by his supplier or by another party. It should be noted that, pursuant to Article 25-octies of the Decree, the offence of receipt of stolen goods may also give rise to the administrative liability of Entities.

Infringement of the freedom of commerce or industry (Article 513 of the Criminal Code)

This offence, prosecutable on the injured party's action, is committed by the exercise of violence against property or the use of fraudulent means to prevent or disrupt the operation of an industry or commerce, unless a more serious offence is committed (e.g. arson, or one of the computer crimes set out in Article 24-bis of the Decree). For instance, this offence has been deemed to occur by those who enter in their website's source code – for the

[74] The Intellectual Property Code (Legislative Decree No. 30/2005), states in Article 2: "*Patenting and registration give rise to intellectual property rights. The following can be covered by patents: inventions, utility models, new varieties of plants. The following can be registered: marks, designs and models, and topographies of semiconductor products*".

purpose of enhancing its visibility for search engines – keywords referable to a competitor's enterprise or products, in order to divert such competitor's potential customers.

Illegal competition through threats or violence (Article 513-bis of the Criminal Code)

This offence occurs when a businessperson carries out acts of competition using violence or threats. This provision introduced into the Criminal Code by the anti-mafia law "Rognoni – La Torre" 646/1982, can also apply outside the scope of mafia-type criminal associations; its purpose is to combat acts aimed at preventing or limiting the market activities of competitors. The offence also occurs when the violence or threat is committed by third parties on behalf of the businessperson, or is not directly directed at the competitor but rather at his potential customers. The offence could, for instance, be committed in the following cases: threatening to cause unjust damage to participants in a public tender in order to learn about their bids and formulate lower bids; threatening, in the relationship with one's own supplier, not to place further orders in the event that the same supplier supplies a particular competitor.

Fraud against national Industries (Article 514 of the Criminal Code)

This offence occurs when harm is done to national industry by placing on sale or otherwise putting into circulation, industrial products with counterfeited trademarks or distinctive marks. The scope of the damage must be such as to harm not only individual enterprises, but the whole industrial economy of Italy.

Fraud in the conduct of commerce (Article 515 of the Criminal Code)

Unless the conduct gives rise to an offence of fraud, this offence is committed by a person engaged in commercial activity who delivers goods other than those agreed, or delivers goods which, while being of the same species as the agreed upon goods, differ from them as to origin, provenance, quality or quantity.

Sale of non-genuine foodstuffs as genuine (Article 516 of the Criminal Code)

The offence is committed by any person who sells or places on the market non-genuine foodstuffs, i.e. substances, foods and beverages intended for human consumption which, while not hazardous for health, have been altered by adding or removing elements, or have a different composition from that required.

Sale of industrial products with deceptive marks (Article 517 of the Criminal Code)

This offence is committed by placing for sale or otherwise putting into circulation intellectual works or industrial products bearing names, trademarks or distinctive marks[75] likely to mislead the buyer about the origin, provenance or quality of the work or product. The offence occurs where the distinctive marks, also having regard to the other circumstances of the concrete case (price of the products, their characteristics, manner of placing for sale) are likely lead the consumers to confuse the products with similar products (but of different origin, provenance or quality) bearing a genuine mark. The provision safeguards correct commercial practices and is applicable in the alternative, where the conditions for the more serious offences set out in Articles 473 and 474 of the Criminal Code are not met. It includes cases such as the counterfeiting and use of non-registered trademarks, the use of or packages with original trademarks but containing different products, and the use of the trademark by the lawful trademark holder on products whose quality standards differ from those of the products originally bearing the trademark (the conduct does not constitute an offence where production is contracted to another company but the client controls compliance with his quality specifications).

Manufacture and sale of goods made by usurping industrial property rights (Article 517-ter of the Criminal Code)

The offence covers two different types of conduct. The first, prosecutable on the injured party's action, occurs when any person, being able to learn of the existence patents or registrations held by other parties, manufactures or uses for industrial manufacturing purposes items or other goods, thereby usurping or violating an industrial property right. If the conduct includes the counterfeiting of trademarks or another of the conducts laid down in Articles 473 and 474 of the Criminal Code, the perpetrator might also be prosecutable for such offences.

The second type of offence occurs when a person, in order to make a profit, introduces in the territory of Italy, holds for sale, places for sale or otherwise puts into circulation goods manufactured in infringement of industrial property rights. If the goods bear counterfeit marks, Article 474, paragraph 2, of the Criminal Code shall also apply.

Counterfeiting of geographical indications or denominations of origin of agricultural food products (Article 517-quater of the Criminal Code)

This offence consists in counterfeiting and altering geographical indications or designations of origin of agricultural food products[76] and, for the purpose of making a profit, introducing

[75] Article 181-bis, paragraph 8, of Law No. 633/1941 states that for the purposes of criminal law the SIAE mark is considered a distinctive mark of an intellectual work.

[76] Pursuant to Article 29 of Legislative Decree No. 30/2005 the following are protected: "*geographic indications and designations of origin which identify a country, region or locality, when they are adopted to designate a product that originates from such places and whose quality, reputation or characteristics are exclusively or essentially linked to the geographical environment of origin, inclusive of natural, human and traditional factors*".

in Italy, holding for sale, offering for sale and offering directly to consumers or putting into circulation such products bearing counterfeit indications or designations.

Making available protected intellectual works in telecommunications networks without authorisation (Article 171, paragraph 1 point a-bis, Law No. 633/1941)

Aggravated unauthorised use of protected intellectual works (Article 171, paragraph 3, Law No. 633/1941)

The first offence occurs when any person, without being authorised, for any purpose and in any form, makes available to the public a protected intellectual work, or a part thereof, by placing it in a system of telecommunications networks through connections of any kind. In certain specific cases – for cultural purposes or purposes of free expression and information, and subject to certain limitations – it is permissible to disclose others' intellectual works to the public[77].

The second offence consists of the unauthorised use of others' intellectual works (by means of reproduction, transcription, dissemination in any form, placing for sale, placing on telecommunications networks, public performance or representation, creative uses such as translations, summaries, etc.); this offence is aggravated by the harm to the author's non-material rights. In this case, the conduct which already constitutes an offence is aggravated by the prohibition of publication imposed by the author, or by usurping authorship (plagiarism), or by deforming, altering or otherwise changing the work in a way that harms the author's honour or reputation.

Both of the above offences apply in the alternative when the conduct is not characterised by profit-making aims, in which case the conduct would be punished, more severely, under the types of offence set out in Articles 171-bis and 171-ter.

Abuses concerning software and databases (Article 171-bis of Law No. 633/1941)

The first paragraph of the Article, which refers to computer software[78], punishes the conducts of unauthorised duplication and import, distribution, sale, holding for commercial or business purposes (hence also for internal use within one's undertaking) and leasing, when such conducts concern software contained in media not bearing the SIAE mark (Italian Society of Authors and Publishers). This offence also occurs when a person prepares, holds or exchanges any means aimed at removing or circumventing software protection devices.

[77] See, for instance, Article 65 of Law No. 633/1941, which provides that current event features published in magazines and newspapers may be used by third parties, unless their reproduction has been expressly forbidden, provided their source, date and author are indicated.

[78] Pursuant to Article 2, No. 8 of Law No. 633/1941 computer software in any form is protected, as long as it is original, which are an intellectual work of their author. The term software includes the preparatory materials for designing such software. Articles 64-bis, 64-ter and 64-quater of the above-mentioned law regulate extension of the software author's rights and cases where the software may be freely used, i.e. the instances where reproductions or actions on the programme are permitted even without the right-holder's specific authorisation.

The second paragraph, which concerns protection of a database author's copyright[79], punishes the permanent or temporary, total or partial reproduction of such database, by any means and in any form – on media not bearing the SIAE mark, and its transfer onto another medium, its distribution, public communication, presentation of demonstration, if not authorised by the copyright holder. This offence also covers the conduct of duplicating and reusing all or a significant part of the database contents, thereby infringing the prohibition imposed by the establisher[80] of the database. "Duplicating" means a permanent or temporary transfer of data onto another medium, by any means and in any form; "reusing" means any form of making the data available to the public, including by distributing copies, rental, or transmission by any medium and in any form.

All the above-mentioned conducts must be characterised by the specific intention of making a profit, i.e. achieving an advantage, which may also consist of saving costs.

Abuses concerning audiovisual or literary works (Article 171-*ter* of Law No. 633/1941)[81]

This provision lists a long series of unlawful conducts – where committed for non-personal use and for profit-making purposes – concerning: works intended for television, cinema, sale or hire; disks, tapes or similar media or any other media containing audio clips or video clips of musical, film or similar audiovisual works or sequences of moving images; literary, dramatic, scientific or educational works, musical or musical drama works or multimedia works. The punished conducts include:

- unauthorized duplication, reproduction, transmission or public dissemination using any procedure;
- the following conducts, engaged in by a person who did not take part in the unauthorised duplication or reproduction: introducing in Italy, holding for sale or distribution, placing on sale, supplying, screening in public or broadcasting on television or radio, or playing in public the unauthorised copies or reproductions;
- the same conduct listed in the above bullet point (except for introducing in Italy and playing/screening in public) is punished when it involves the use of any media – even

[79]Under Article 2, No. 9, of Law No. 633/1941, databases consist of collections of works, data or other independent elements, systematically or methodically arranged and which can be accessed by individuals using electronic or other means. This provision clearly leaves unprejudiced the separate protection granted to any copyright existing on intellectual works which may be present in the database. Articles 64-quinquies and 64-sexies of the law regulate the extension of the database author's copyright and the cases where the database can be freely used.

[80] The right of the establisher of the database are regulated by Articles 102-bis and 102-ter of Law No. 633/1941. The word "establisher" designates the party who made substantial investments in order to create, verify or presenting a database and who, independently of the protection granted to the database author in respect of the creative criteria according to which the material was selected and arranged, has the right to forbid the duplication or reuse of all or a significant part of the database contents. With regard to databases available to the public, for example by means of free online access, the users, also without the establisher's express authorisations, may duplicate or reuse non-significant parts of such databases' contents, in qualitative and quantitative terms, for any purpose, except where such duplication or reuse have been expressly forbidden or limited by the establisher.

[81] Article amended by Law No. 93/2023.

when not obtained by unauthorised duplication or reproduction – not bearing the required SIAE mark or which bears a counterfeit mark.

The following abuses are also prosecutable: the dissemination of services provided with unscramblers of encrypted transmissions; the trafficking in devices which enable unauthorised access to such services or products aimed at circumventing the technology safeguards preventing unauthorised uses of protected works; removing or altering electronic copyright notices present in the protected works or appearing in notices to the public; or importing or putting into circulation works from which the above-mentioned copyright information has been deleted or altered; storing on a digital, audio, video or audiovisual medium, in whole or in part, a cinematographic, audiovisual or editorial work – even if carried out in places of public entertainment – or reproducing, executing or communicating to the public the improperly stored material.

Failure to make communications or making false communications to SIAE (Article 171-septies of Law No. 633/1941)

This offence is committed by any manufacturers or importers of media containing software intended for sale who fail to provide SIAE with the data necessary to identify the media in respect of which they wish to avail themselves of exemption from the obligation to affix the SIAE mark[82].

The offence also includes providing a false declaration of compliance with legal obligations to SIAE in order to obtain the SIAE marks to be placed on the media containing software or audiovisual works.

Fraudulent unscrambling of restricted-access transmissions (Article 171-octies Law No. 633/1941)

This offence is committed by any persons who, for fraudulent purposes, produces, imports, distributes, installs, places on sale, modifies or uses, also for personal use only, devices for unscrambling restricted access audiovisual transmissions, also where these are receivable free of charge.

Smuggling crimes (Legislative Decree No. 43/1973).

These provisions punish a structured set of behaviour which, in brief, has the aim of avoiding paying border duties on goods.

[82] Under Article 181-bis, paragraph 3 of Law No. 633/1941, without prejudice to compliance with the rights protected by the law, the SIAE mark need not be affixed to media containing software to be used solely via a computer and not containing any audiovisual works other than works created expressively for the computer software, and not containing reproductions exceeding 50% of pre-existing audiovisual works, giving rise to competition in their use for profit-making purposes.

Border duties mean import and export duties, levies and other taxes on exports or imports required under EU regulations, monopoly rights, border surcharges and any other consumption tax or surcharge in favour of the State.

7.9.2 Sensitive company activities

With reference to the Company's operations, the risks of commission of offences against industry and trade and copyright infringement are particularly limited. Potentially, the Company could be a party to such offences as a result of its stake in companies involved in the illegal activities in question. However, conducting a thorough analysis of the target companies leads to an in-depth knowledge of the counterparty such as to avoid establishing relations with parties that do not provide sufficient guarantees as to the propriety of their actions.

Further sensitive activities are likely to occur:

- in participation in public tenders, with particular reference to unlawful conduct towards participants (e.g. unlawful competition with threats and violence);
- in the procurement or use of products, software, databases and other intellectual works to be used in Company activities or intended as gifts.

A lower degree of risk is associated with the development and launch of new products, with management of the Company’s naming and trademarks, external communication or advertising and marketing initiatives, or with customer relationship management based on the principles of fair competition and correct and transparent commercial practices, and this by reason of the well-developed system of safeguards and control procedures already laid down in the sectorial legislation.

Taking into account what is specified in this chapter, reference is therefore made to the following protocols:

- “Financial fight against terrorism and money laundering of the proceeds of crime” - Chapter 7.4.2.1;
- “Management of the procedures for the procurement of goods and services and for the appointment of professional consultants - Chapter 7.2.2.6;
- “Management of gifts, entertainment expenses, donations to charities and sponsorships” - Chapter 7.2.2.7; from here
- “Management and use of IT systems and Information assets” - Chapter 7.8.2.1;
- “Signing contracts with the Public Administration” - Chapter 7.2.2.1;

which contain processes, control principles and principles of conduct also aimed at preventing the commission of the offences referred to in this chapter.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

With regard to smuggling crimes, the risks of committing said may arise in the context of the Asset Management Company's activities relative to processes for the procurement of any imported goods, as well as of a more general nature in obligations with the customs authorities. Accordingly, reference is made to the applicable protocols:

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.10 Sensitive area concerning environmental crimes

7.10.1 Type of offence

Article 25-undecides of Legislative Decree No. 231/2001 identifies offences against the environment, for which, based on Community law provisions, entities are administratively liable[83].

These offences are described in the Italian Criminal Code, in Legislative Decree No. 152/2006 (Environment Protection Policy, hereinafter referred to as EPP) and in various special laws, both classified as criminal offences as well as contraventions[84]. These cases are the following:

Environmental pollution (Article 452-*bis* of the Criminal Code)

The regulation punishes all those who unlawfully endanger or bring about a significant and measurable deterioration of water, of air, of the soil or subsoil, of an ecosystem or of the biodiversity.

Environmental disaster (Article 452-quater of the Criminal Code)

The regulation punishes all those who unlawfully provoke an environmental disaster, that consists in the irreversible alteration of the equilibrium of ecosystem, or the elimination of which is particularly burdensome and exceptional, or in harm to public safety based on the severity of the event, the extension or effects, or due to the number of persons harmed or exposed to hazard.

Traffic and abandonment of highly radioactive material (Article 452-sexies of the Criminal Code)

Diverse unlawful conduct (disposal, purchase, receipt, transport, import, export, detention, abandonment, etc.) involving highly radioactive materials is punished.

Criminal association with aggravating circumstances regarding the environment (Article 452-octies of the Criminal Code)

The regulation anticipates specific aggravating circumstance for the penalty for crimes of criminal association having the goal of committing any of the environmental offences provided for by the Criminal code. If involving a “mafia-type association”, the fact itself of

[83] Article 25-*undecies* of Legislative Decree No. 231/2001, in force since 16 August 2011, in the text first included in Legislative Decree No. 121/11 enacted for the application of Directive 2008/99/EC and Directive 2009/123/EC, and subsequently amended by Law No. 68/15, in force since 29 May 2015, that introduced new environmental crimes in the Criminal Code

[84] The offences are those provided for by the Criminal Code (except for Articles 727-*bis* and 733-*bis*) and by the EPP in Articles 258, 2nd sentence, paragraph 4, 260, paragraphs 1 and 2, 260-bis, paragraphs 6, 7 and 8, and document forgery to trade in animal and plant species and the offence of wilful pollution by ships. As a general rule, the essential elements of a crime are punished even if committed work orders by way of negligence; the crimes of pollution, contamination and environmental disaster, if committed through negligence, are punished pursuant to Article 452-*quinquies* of the Criminal Code and constitute and also constitute predicated crimes with administrative liability for Entities.

acquiring the management or control of an economic activity, of concession, of authorizations, authorisations, public tenders, or of public services regarding environmental matters is an aggravating circumstance.

Offences involving protected wild animals or plants or protected habitats (articles 727-bis and 733-bis of the Criminal Code)

The capture, possession, killing or destruction of specimens pertaining to species of protected wild animals or plants shall be punishable, excluding cases where this is allowed by law or where the damage is considered negligible in terms of the quantity of specimens involved or in terms of the impact on the preservation of the species. Also punishable is destruction or damage that endangers the conservation status of a habitat inside a protected site. Community rules list the protected animal and plant species and identify the characteristics which impose that local laws classify a natural habitat or the habitat of species as a special protection area or special area of conservation.

Breach of rules regulating discharges (Article 137, paragraphs 2, 3, 5, 11 and 13, EPP)

Article 137 EPP punishes a series of violations of the rules on waste water, and in particular: unauthorised discharges of industrial waste water containing specific hazardous substances, or in contravention of the provisions contained in the authorisation or notwithstanding its suspension or revocation, and discharges of hazardous substances beyond the established limits; breach of discharges restrictions on the ground, in groundwater and underground, except in the cases contemplated under articles 103 and 104 EPP.

Lastly, breach of rules prohibiting discharges into sea of hazardous substances by ships or aircrafts, as defined in international treaties is also punishable, save for authorized discharges of rapidly biodegradable quantities.

Breach of waste management regulations (Article 256, paragraphs 1, 3, 5 and 6, 1st part, EPP)

Punishable deeds are waste collection, transport, retrieval, disposal, sale or brokerage in the absence of the necessary licences, enrolment in the national Register of waste management bodies and notification to the competent authorities or in contravention of provisions included in the licences issued or communicated by the authorities or in the absence of the applicable requirements.

Moreover, unauthorised activities involving the creation or management of a waste tip, mixture of different types of hazardous waste either amongst themselves or with waste

which is not hazardous and the deposit of hazardous medical waste at the place of production of a quantity exceeding 200 litres, or equivalent quantity, are also punishable.

Failure to conduct remediation for cases of ground, underground, surface water or groundwater pollution (Article 257, paragraphs 1 and 2, EPP)

Unless the fact constitutes a more serious crime (e.g. referred to above in Article 452- *bis* of the Criminal Code), anyone who has caused the pollution in question by exceeding the risk threshold concentrations and does not arrange for the necessary communications to the competent authorities and the clean-up of the site pursuant to Article 242 of the EPP is liable to be punished. Clean-up actions are a condition of non-punishment also for the environmental fines envisaged by other special laws for the same event.

False certification of waste analysis (Article 258, paragraph 4, 2nd part, EPP) [85]

Whosoever provides false information on the nature, composition and chemical-physical properties of waste shown on the waste analysis certificate and whosoever utilises a false certificate for the transport of waste shall commit this offence.

Illegal shipment of waste (Article 259, paragraph 1, EPP)

The regulation punishes whosoever makes a cross-border shipment of waste in breach of EU Regulation No 259/93, which was repealed and substituted by EU Regulation No 1013/2006.

Activities organised for the illegal trafficking of waste (Article 452-quaterdecies, paragraphs 1 and 2 of the Criminal Code)

This offence is committed by those who, for illicit gain, sell, receive, transport, export, import or, in any event, wrongfully manage significant quantities of waste. These shall not include sporadic events, but continuous activities for which proper means and organisation have been put in place. Highly radioactive substances shall constitute an aggravating circumstance.

False declaration on the origin of waste for SISTRI (Article 260-bis, paragraph 6 – paragraph 7, 2nd and 3rd part – paragraph 8, EPP) [86]

[85] Article 4 of Legislative Decree No. 116/2020 reformulated Article 258 of the EPP starting from 26 September 2020, with the consequence that the second part of paragraph four, which still refers to Article 25-undecies of Legislative Decree No. 231/2001 provides for a different case, concerning the transport of hazardous waste without waste disposal records, while the offence described herein is now in the third part of the same paragraph. It is therefore considered that due to the oversight of the legislator, it can be argued that neither the new nor the original crime could constitute a predicate offence.

Producers of waste and other persons involved in its management (sellers, brokers, collection or recycling consortia, persons undertaking collection or disposal operations) must participate or volunteer to participate in the IT system of control on the origin of waste known as SISTRI, according to criteria in Article 188-ter of the EPP. In this respect, offences consisting in providing false information on the nature and characteristics of waste in order to obtain a waste analysis certificate to be entered in SISTRI, entering a false certificate in the system and using such certificate for the transportation of waste shall also be punishable.

The transport operator that uses a fraudulent hard copy of a SISTRI form, filled in for shipment of waste, is also punishable.

Breach of the regulations governing atmospheric emissions (Article 2, paragraph 5, EPP)

This regulation punishes emissions into the atmosphere resulting from factory operations which exceed the limits established by law or as fixed in the licenses or regulations issued by the competent authorities and when they exceed the limits prescribed to ensure good quality of air in terms of current regulations.

Breach of regulations governing sale and detention of animals or plants which are in extinction or of dangerous mammals or reptiles (Law No. 150/1992, Article 1, paragraphs 1 and 2 – Article 2, paragraphs 1 and 2 – Article 3-bis paragraph 1 – Article 6, paragraph 4)

Offences consist in the import, export, transport and retention of animals and plants in breach of Community and international regulations which prescribe special permits, licenses and customs certificates, and false declarations or alteration of the above documents. The detention of certain dangerous mammals and reptiles is likewise prohibited.

Substances detrimental to the ozone layer (Law No. 549/1993, Article 3, paragraph 6)

The law prohibits trade, use, import, export and retention of substances which are detrimental to the ozone layer as listed in the same law.

Pollution from ships (Legislative Decree No. 202/2007, articles 8 and 9)

Save as otherwise provided, this rule forbids commanders of ships, members of the crew, owners and ship builders from wilfully or negligently pouring into the sea hydrocarbons or harmful liquid substances transported in an improper manner.

[86] As from 1.1.2019, the waste disposal management register SISTRI has been abolished by Article 6 of Decree-Law No. 135/2018, which has introduced a new waste traceability system (REN), with implementing provisions still to be completed.

7.10.2 Sensitive company activities

With reference to the company's operations, the risks of environmental offences being committed are very limited. We cannot, however, exclude risks of committing illegal deeds concerning the production of waste, discharges, atmospheric emissions and ground pollution. In this regard, it should be noted that Neva has its registered office and operating offices in buildings leased from third-party owners, the maintenance of which is the responsibility of the owner, and operating offices in buildings belonging to the Banking Group, the maintenance of which is managed by the competent operating unit of the Parent Company.

The protocol dictating the control principles and rules of conduct applicable to the management of environmental risks, consistent with the outsourcing contract in place with Intesa Sanpaolo SpA (service provider), is set out below.

Please also refer to the protocols:

- “Management of activities connected with the application for authorisation or the implementation of obligations vis-à-vis the Public Administration” in paragraph 7.2.2.3.;
- “Management of the procedures for the procurement of goods and services and for the appointment of professional consultants” in paragraph 7.2.2.7;

which include principles of control and conduct aimed at avoiding offences defined in this Chapter.

Such protocols also apply to the monitoring of any activities performed by Group companies and/or outsourcers on the basis of special service agreements.

7.10.2.1 Environmental risk management

This protocol applies to all the Structures involved in the management of environmental risks and to the external Companies in charge of the activities.

In compliance with its Code of Ethics which identifies protection of the environment as a key value, the Intesa San Paolo Group has adopted a specific environmental policy, which must be disseminated, understood and adopted at all levels of the organisation.

In addition, the Intesa Sanpaolo Group has adopted and maintains an Environmental and Energy Management System, which is verified annually by an international Certification Body, conforming to applicable laws and the most up-to-date reference standards: UNI EN ISO 14001 and UNI CEI EN 50001.

The company avails itself of Intesa Sanpaolo's specialist structure (outsourcer for such activities) which ensures the technical skills and powers necessary for the verification, assessment, management and control of risk.

The corporate Structures in charge of managing environmental documentation, including authorisations and certifications issued by the Public Administration, must comply with the rules of conduct set out and described in the protocol "*Management of activities relating to applications or the fulfilment of requirements with the Public Administration*".

The purpose of this protocol is to ensure compliance, by the Company and the external companies appointed, with current legislation and the principles of transparency, fairness, objectivity and traceability in the performance of the activities in question.

Process description

First of all, it should be emphasised, as noted above, that Neva SGR does not own any real estate; its headquarters and operating offices are located in the city of Turin at third-party rented properties, and in the cities of Bologna and Rovigo at Group-owned properties.

The waste management and plant maintenance activities of the Group's buildings are outsourced to the Parent Company, which in turn may subcontract these activities to third parties. The service contract with the Parent Company also includes routine and scheduled maintenance for environmental hygiene (cleaning, supply of sanitising materials, special waste management pursuant to the Environmental Code, i.e. Legislative Decree No. 152/2006).

Any special waste generated by the renovation of the premises, as provided for in the contracts, shall be managed with costs borne by the contractor (Parent Company on behalf of the owner) in accordance with the regulations in force.

With respect to environment risk, reference is made to the following processes:

Management of legal obligations governing waste:

Management of expenses and purchases:

- Purchase cycle;
- Delivery management;
- Sourcing.

That being said, Neva currently manages the disposal of part of the waste, in accordance with current regulations and the separate collection system.

Specifically:

- all offices in the different cities are equipped with special waste collection containers;
- waste disposal is the responsibility of the landlord (for the Turin offices) and the Building Managers (for the Bologna and Rovigo offices)
- with regard to the Group's properties, disposal is carried out through companies contracted by the Parent Company.

The operating terms for management of these processes are governed by internal regulations, developed and updated by the competent Structures, which constitute an integral and essential part of this protocol.

Control principles

Without prejudice to the provisions of the Parent Company's regulations for the activities managed by the Parent Company, below are the control principles relating to the activities managed by Neva.

- Authorisation levels defined within the process:
  - with respect to the purchase of goods and services, approval of the purchase request, appointment, signature of the agreement and issuing of orders shall be undertaken exclusively by persons duly empowered in terms of the system regulating assignment of powers and appointments in force which establishes the individual management powers by nature of expense and duty involved. The internal set of rules illustrates these authorisation mechanisms, and indicates the corporate officials who hold the necessary powers;
  - all transportation of special waste must be accompanied by an identification form signed by the transport operator and, as far as the Company is concerned, by persons duly appointed for this purpose;
  - assignment to third parties – by suppliers of the Company – of sub-contracted activities is contractually subject to the prior approval of the Company structure which has stipulated the agreement and in compliance with the specific obligations in fulfilment of environment regulations.
- Separation of duties amongst the different persons involved in the environment risk management process. Specifically:

- the operating Structures which are responsible for creating and managing activities involving services to individuals, buildings, maintenance, building and plant installation projects and other integrated services (e.g. toner supply, management of dispensaries, management of distributed IT equipment, controls/reconditioning/disposal of IT materials or products, etc.) are separate and distinct from the Structures responsible for consultancy on the evaluation of environmental risks and on monitoring the measures suited to prevent and limit them.

- Control activities:
  - where applicable, the special waste identification form completed and signed by the transporter must be verified by the person appointed by the Company;
  - sample checks on proper management of waste particularly special waste and, if present, hazardous waste carried out by the competent structures;
  - review of the proper management of waste by the contractor resulting from ordinary and extraordinary maintenance and from building restructuring. More specifically, the contractor is bound to retrieve all "refuse" accumulated during its work cycle and the Managers or persons duly appointed by the Operating Units where the works are carried out must inspect that the contractors have properly performed their duties ensuring that no waste products are left within the Company premises;
  - monitoring the proper implementation, by suppliers, of maintenance/cleaning services (for buildings and persons, etc.) with particular attention to the proper upkeep of maintenance logs for climate control systems, as well as regular maintenance reports drawn up by suppliers to whom said services have been subcontracted (e.g. reports on "leakage test" of reservoirs for storage of fuel).
- Process traceability including both the electronic and the paper trail:
  - use of IT systems supporting the operations, to ensure that the data and information relating to the procurement process are recorded and kept on file;
  - documenting all activities related to the process with particular reference to the proper upkeep and maintenance logs for climate control systems, in compliance with provisions of applicable legislation, particularly regarding emissions;
  - retention within the legal deadlines (five years from the last registration) of the special waste identification form (where applicable) and the loading and unloading register for hazardous waste;
  - in order to allow a clear understanding of the responsibilities and the motives behind the choices made, the Structure of the company in charge from time to time involved shall be responsible for archiving and preserving the documentation produced also

by electronic means, in relation to the execution of the duties fulfilled in compliance with the above described processes.

Rules of conduct

All the Company's operating units, in whatever capacity involved in the management of environmental risks, as well as all employees, are required to comply with the procedures set out in this protocol, the existing legal provisions on the subject, the internal regulations and any provisions of the Group's Code of Ethics and Internal Code of Conduct.

In particular, all operating units are required – in their respective areas – to:

- monitor, to the extent of their competence, compliance with environmental requirements, in particular compliance with the operational rules on the grouping and temporary storage of waste according to its classification, delivery to designated transporters and the management of boilers and refrigeration units;
- refrain from granting appointments/assignment of work to external consultants and/or suppliers in breach of the documented criteria and objectives aimed at ensuring professionalism and expertise, competitiveness, price, integrity and ability to guarantee an efficient assistance. In particular, the rules for the selection of professionals shall refer to the criteria of clarity and availability laid down in the Group's Code of Ethics and Internal Code of Conduct;
- in the event that the involvement of third parties is envisaged for the management/prevention of risks, the agreements with these third parties must include a declaration of awareness of the regulations set under Legislative Decree No. 231/2001 and an undertaking to comply therewith;
- include, in supply, work and Service Supply Agreements for People, Building maintenance, building/plant works and other integrated services (e.g. toner supply, management of dispensaries, management of distributed IT equipment, controls/reconditioning/disposal of IT materials or products, etc.), specific clauses on compliance with environmental regulations;
- in terms of the purchase procedures applicable to products, machinery and tools, which at the end of their life cycle could be classified as potentially hazardous to the environment, the contracting Structures and the competent purchasing function must first obtain the "product hazard classification/material safety datasheet" and the EWR codes", and all information necessary for their correct disposal;
- consider environment certifications as a vital requisite for evaluating the supplier, where the nature of the supply makes this possible and opportune;

- adopting a transparent and collaborative stance with respect to controlling Entities (e.g. The Social Security Department (ASL), The Fire Department, ARPA, The Municipal Authorities, The Province Authorities, etc.) in the event of checks/inspections.

Likewise all employees shall:

- comply with legal provisions and internal regulations and directives given by the company's Structures and the competent Authorities;
- immediately report any environmental emergencies (e.g. fuel spills, serious plant malfunctions causing external noise exceeding the limit values) to the Building Manager and/or the emergency management staff or the landlord.

In any case, it is forbidden to engage in conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- provide incomplete documentation and/or communicate false or modified data;
- use deceit which could lead Public Bodies in error;
- deposit waste outside the "Temporary Landfill" and hand over special waste, as defined in the current internal regulations, to suppliers appointed to transport the same which are not included in the list of Companies authorised to manage waste available on the company intranet.

7.11 Sensitive area concerning tax crimes

7.11.1 Type of offence

The liability of entities is extended to some of the offences relating to income tax and value added tax provided for by Legislative Decree No. 74/2000, which sets out general rules on tax crimes, in order to strengthen the repression of the phenomenon of tax evasion and to implement the provisions of European legislation aimed at protecting the interests of the public finance of the Union.

New tax crimes have been included in Article 25-quinquiesdecies[87]. The offences in question are described below.

Fraudulent statement through the use of invoices or other documents for non-existent transactions (Article 2, Legislative Decree No. 74/2000)

Fraudulent statement through other artifices (Article 3, Legislative Decree No. 74/2000)

The first offence is committed by entities that file income tax or VAT tax returns that indicate fictitious payable items, resulting from invoices or other documents recorded in mandatory accounts or kept as evidence. The invoices or documents used refer to material falsification or provision of intentionally false statements concerning all or part of the transactions indicated, or regarding the counterparty.

The second crime exists if, apart from the use of invoices or documents certifying non-existent transactions as above, one of the aforesaid returns indicates amounts receivable below actual amounts, or fictitious payable amounts, receivables and withheld amounts, through transactions that are objectively or subjectively simulated, or using false documents, recorded in mandatory accounts or kept as evidence, or misrepresenting accounting, obstructing assessments or misleading the Tax Authorities. This crime does not exist if certain thresholds are not exceeded, or the misrepresentation is not attained through artifice, but simply due to the omission of invoicing and registration obligations, or by only indicating in returns items receivable which are below actual amounts receivable.

[87] Legislation on tax crimes was reformed by Decree-Law No. 124/2019, of which Article 39 introduced tax crimes to Legislative Decree No. 231/2001, with effect from 24 December 2019. Article 5 of Legislative Decree No. 75/2020 then added the crimes of omitted or untrue statements and undue compensation, and made punishable – by amending Article 6 of Legislative Decree No. 74/2000 – the declaratory crimes referred to in Articles 2, 3 and 4 only if attempted, with effect from 30 July 2020.

Both offences are formalised with the submission of the declarations and are also punishable by way of attempt[88], pursuant to Article 6 of Legislative Decree No. 74/2000, apart from cases of complicity in the offence of "issuing invoices or other documents for non-existent transactions" (Article 8 of Legislative Decree No. 74/2000), if the conduct is carried out for the purpose of evading value added tax within the framework of cross-border fraudulent schemes, connected to the territory of at least one other Member State of the European Union, from which a total loss of EUR 10 million or more results or is likely to result.

Inaccurate tax return (Article 4 of Legislative Decree No. 74/2000)
Omitted tax return (Article 5 of Legislative Decree No. 74/2000)
Undue compensation (Article 10-quater of Legislative Decree No. 74/2000) FROM HERE

These offences punish those who:

- in annual VAT returns indicate assets for an amount below the actual amount, or non-existent liabilities, and certain thresholds of criminal relevance have been exceeded;
- do not file, and have the obligation to do so, a return relating to such taxes (or the return of the withholding agent) when a certain tax threshold has been exceeded;
- do not pay taxes due using unpaid credits as compensation, for an annual amount exceeding a certain threshold.

Such criminal conducts also entail administrative liability pursuant to Legislative Decree No. 231/2001 only if it concerns the evasion of VAT in the context of cross-border fraudulent systems connected to the territory of at least one EU Member State and if, as a result of the commission of such offences, damage of €10 million or more in total results or is likely to result.

In the presence of both circumstances, the offence of misrepresentation is punishable, pursuant to Article 6 of Legislative Decree No. 74/2000, even if it is only attempted, that is to say, when there are preparatory acts, such as the omission of invoicing obligations, which may therefore have an effect on the subsequent declaration, if those acts are also carried out in the territory of another EU Member State if the conduct is carried out for the purpose of evading value added tax as part of cross-border fraudulent schemes, connected to the territory of at least one other EU Member State, from which a total loss of EUR 10 million or more results or may result.

[88] Please note that pursuant to Article 26 of Legislative Decree No. 231/2001, the liability of entities for attempted offences does not exist if the entity voluntarily prevents the completion of the action or the occurrence of the event.

Issue of invoices or other documents for non-existent transactions (Article 8, Legislative Decree No. 74/2000)

Subjects that, in order to enable third parties to evade income taxes or VAT, issue or provide invoices of other documents for non-existent transactions, commit a crime.

The subject issuing invoices or documents and party committing this crime cannot be punished for aiding and abetting a fraudulent statement of the third party that uses such documents, and similarly the third party cannot be punished for aiding and abetting the crime of issuing the invoices or documents.

Concealment or destruction of accounting documents (Article 10, Legislative Decree No. 74/2000)

This crime is committed by anyone who, in order to evade income taxes or VAT or that enables third parties to evade, conceals or destroys in whole or in part accounting records or documents which must be retained, so as to prevent the reconstruction of income or business turnover.

Fraudulent omission of tax payments (Article 11, Legislative Decree No. 74/2000)

The punished conduct involves carrying out simulated or fraudulent acts on own or third-party property, which can invalidate the procedure to collect income tax and VAT, interest or administrative fines relative to such taxes, for a total amount of more than 50 thousand euro.

The conduct of anyone who, as part of a tax transaction, in order to obtain for themselves or others the reduced payment of taxes and additional items, indicates in filed documents amounts receivable that are lower than actual amounts or fictitious payable amounts for a total amount of more than 50 thousand euro, will also be punished.

7.11.2 Sensitive company activities

The risk of committing tax crimes is possible in all company activities. It is specifically governed by the protocol "Management of risks and obligations for the prevention of tax crimes".

As regards the Company's position as taxpayer, this risk is also governed by the protocol "Management of periodic reporting". The following should also be considered:

- the Company has joined the cooperative compliance scheme with the Tax Authorities contemplated in Article 3 of Legislative Decree No. 128/2015 and has adopted for this purpose a system to identify, measure, manage and control tax risk, described in the

"Guidelines to manage tax risk in the cooperative compliance scheme with the Tax Authorities" and in other sources of detailed company regulations;

- the Parent Company Intesa Sanpaolo exercised, as of 1 January 2019, the option to form a VAT Group as governed by Title V-bis of Presidential Decree No. 633 and the related implementing decree Ministerial Decree 6 April 2018. Participation in a VAT Group entails a single (new) tax entity being set up, as the VAT Group: i) has a single VAT number, ii) operates as a single VAT taxable subject in relations with entities not belonging to the group, iii) fulfils all obligations and exercises all relevant rights/options (e.g. separation of activities for VAT purposes) for VAT purposes. The VAT group operates through the representative company (Intesa Sanpaolo) which exercises control over the other in-scope companies[89].
- the Parent Company Intesa Sanpaolo has activated, starting from 2004, the National Tax Consolidation, governed by Articles 117-129 of the Consolidated Income Tax Act, which almost all resident companies of the Intesa Sanpaolo Group are party to, on an optional three-year (renewable) basis. As a result of the aforementioned option, each company, including the consolidating company, continues to autonomously declare its income or tax loss, in addition to withholding taxes, deductions and tax credits; these components are understood to be transferred by law to the parent/consolidating company which, in the context of the consolidated tax return (CNM model) (i) determines a single taxable income or a single tax loss that can be carried forward resulting from the algebraic sum of own income/losses and of the consolidated companies, (ii) makes the consolidation adjustments required by law, (iii) deducts the withholdings and own tax credits and those transferred from the consolidated companies, to determine the single IRES payable or credit pertaining to the Tax Consolidation.

As regards relations with third parties, such as customers, suppliers, partners and counterparties in general in order to mitigate the risk of being involved in tax crimes, also in view of the fact that the law, pursuant to Article 13 bis of Legislative Decree No. 74/2000, severely punishes banking and financial intermediaries that take part in the processing or marketing of tax evasion models, the Company has also prepared protocols regulating the following activities:

- Management of the procedures for the procurement of goods and services and for the appointment of professional consultants;
- Management of gifts, entertainment expenses, donations to charities and sponsorships;
- Purchase, management and disposal of investments and other assets;

[89] The regulation requires the mandatory participation ("all-in all-out" clause) of all subjects bound by financial, economic and organisational constraints with the Parent Company.

- Financial fight against terrorism and money laundering of the proceeds of crime;

that contain the principles of control and conduct to observe also for the purposes of preventing tax crimes.

With reference to management of tax risk relating to products and services offered to customers, which concern cases in which the Company could be potentially involved in irregular tax transactions by customers, the discipline is contained in the "Guidelines for the approval of new products, services, start-up of new activities and entering new markets", in the "Guidelines for the approval of new products, services and activities aimed at specific target customers" and in the "Rules for assessing the tax conformity of products, services and transactions proposed to customers".

It cannot be ruled out that the violation of the obligations of notifying the Revenue Agency of the cross-border mechanisms provided for by Legislative Decree No. 100/2020, beyond the specific administrative sanctions envisaged, can be interpreted as an indication of a previous involvement of the Company's appointee in the customer’s fiscal/tax violations, violations which, in this context, in reference to the known conditions of interest or advantage, could, where attributable to predicate offences (of both a both fiscal and money laundering/self-laundering nature), entail liability risks for the Company pursuant to Legislative Decree No. 231/2001. In this regard, Group Rules for the management of the reporting obligations envisaged by DAC 6 (“Directive on Administrative Co-operation”) establish the roles and responsibilities in managing the process to identify and report operations.

Such protocols also apply to the monitoring of any activities performed by Group companies or outsourcers on the basis of special service agreements.

7.11.2.1 Management of risks and obligations for the purposes of preventing tax crimes

This protocol applies to all Company structures involved in managing risks and obligations for the purposes of preventing tax crimes.

The Company has outsourced to an outsourcer outside the Group the administrative/accounting management activities of the Company, as well as the related tax duties, on the basis of a specific contract that regulates, among other things, the communication and operational processes between the various parties involved in the performance of the activities in question.

Pursuant to Legislative Decree No. 231/2001, the process could pose risks of the following tax crimes being committed: "*Fraudulent declaration using invoices or other documents for non-existent transactions*", "*Fraudulent declaration by means of other devices*", "*Issuance of invoices or other documents for non-existent transactions*", "*Concealment or destruction of accounting documents"* and "*Fraudulent evasion of tax payments*", *"Untrue declaration" (Article 4 of Legislative Decree No. 74/2000)¸ "Omitted declaration" (Article 5 of Legislative Decree No. 74/2000), "Undue compensation" (Article 10-quater of Legislative Decree No. 74/2000).*

Moreover, company rules and controls on completeness and truthfulness in this protocol are also prepared in order to enhance actions to prevent crimes that could result in the incorrect management of financial resources, such as "*Money laundering*" and "*Self-laundering*".

As established in "Principles of conduct on taxation", the Company and the Intesa Sanpaolo Group intend to maintain cooperative, transparent relations with the Tax Authorities and promote participation in cooperative compliance schemes.

The contents of this protocol are aimed at ensuring that the Company complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in the performance of the activity in question. It applies to all Structures involved in the management of tax-related risks and to the activities carried out, on the basis of specific service agreements, by other Group companies and/or external outsourcers.

Process description

The process to manage risks and obligations for preventing tax crimes address, directly and/or indirectly, a diverse number of company processes that concern:

- the purchase and sale of goods and services;
- the representation of operations in accounts and company systems;

- the management of obligations concerning invoices payable and receivable, and those relative to the "VAT Group";
- the preparation of tax returns and the correct payment of relative taxes;
- the obligations related to the "Cooperative compliance scheme with the Tax Authorities", which the Company is party to.

The representation of operations in the accounts and company systems, including the evaluation of individual items, is governed by the protocol "*Management of periodic reporting"*.

Relations with the Supervisory Authorities on tax matters (Revenue Agency) are governed by the protocol "*Management of relations with the Supervisory Authorities*".

The operating procedures for management of the processes are governed by the internal rules, which are developed and updated by the competent Structures, and which form an integral and substantive part of this protocol.

Control principles

The control system for monitoring the processes described above must be based on the following elements:

- Authorisation levels defined within the process:
  - all subjects involved in managing activities concerning the preparation of tax returns, and in activities relating to the issue / registration of invoices: are identified and authorised according to the specific role assigned by the Organisational Manual and the Functional Chart or by the Head of the reference Structure by means of internal delegation, to be kept on file by the same Structure;
  - if external consultants/suppliers are involved, they are identified in a letter of appointment, or in contract clauses; only operate within the scope assigned to them by the Head of the reference Structure;
  - each agreement/contract with the Tax Authorities is formalised in a document, duly signed by subjects with suitable powers based on the system of powers and authority adopted;
  - in cases where the tax strategy the Company intends adopting is not agreed by the Tax Authorities, final adoption must be approved by the Board of Directors, after an assessment on the risks and costs/benefits arising from the position the Company wishes to adopt and after an opinion from at least one high-standing external tax consultant.
- Segregation of duties among different persons involved in processes to manage risks and obligations for the purposes of preventing tax crimes. In particular: the activities relating to the different phases of the process must be carried out by different and clearly

identifiable parties/persons, and must be supported by a maker and checker mechanism.

- Control activities:
  - the controls concerning the completeness, correctness and accuracy of the information provided to the tax authorities by the Structure concerned as to the activities falling under its competence that must be supported by maker and checker mechanisms;
  - legal controls on compliance with legislation applicable to tax returns;
  - automated ongoing system controls concerning periodic tax returns;
  - controls on the correct issue, adoption of VAT rates and registration of invoices receivables and their correspondence with contracts and undertakings with third parties;
  - objective and subjective controls on the actual underlying relationship with invoices payable received and on correct registration and accounting.
- Process traceability including both the electronic and the paper trail:
  - each significant phase of the risk management process and obligations for the purposes of preventing tax crimes must be recorded in written documentation;
  - in order to reconstruct the responsibilities and reasons for choices made, each structure is in charge of filing and retaining competent documents produced digitally or electronically.
- Bonus or incentive systems: bonus and incentive systems must be able to guarantee compliance with legal provisions, the principles of this protocol and the provisions of the Code of Ethics, also envisaging suitable corrective mechanisms for any conduct deviating from the norm.

Rules of conduct

The Structures of the Company and of the outsourcer, involved for any reason in managing risks and obligations for the purposes of preventing tax crimes covered by the protocol, are required – like all employees – to observe the procedures indicated in the protocol, applicable legal provisions, internal regulations as well as requirements of the Group's Code of Ethics, Internal Code of Conduct, Administrative/Financial Governance Guidelines, Principles of Conduct on Taxation and Guidelines for managing tax risk in the cooperative compliance scheme with the Tax Authorities. In particular, all Structures shall – in their relevant fields:

- guarantee the true and fair representation of financial data in the Company's tax returns;

- comply with principles of conduct on taxation, in order to: (i) guarantee conformity over time to the tax legislation of countries where the Company operates and, (ii) the financial integrity and reputation of all Group Companies;
- act based on values of honesty and integrity in managing the tax variable, aware that income from taxes constitutes one of the main sources that contributes to the economic and social development of countries where the Company operates;
- guarantee the fostering of a company culture based on values of honesty and integrity and the principle of lawfulness;
- maintain cooperative, transparent relations with the Tax Authorities, guaranteeing that the Authorities have a full understanding of facts behind the adoption of tax regulations;
- meet tax obligations according to the times and procedures defined by regulations or the tax authorities;
- avoid types of tax planning that may be considered as aggressive by the tax authorities;
- interpret regulations according to their intent and purpose, without any exploitation of their literal formulation;
- represent acts, facts and negotiations undertaken in such a way that applicable tax regimes may be applied that conform to the actual economic substance of the transactions;
- guarantee the transparency of operations and the determination of income and assets, avoiding the use of structures, also corporate, that may conceal the actual beneficiary of the income flows or ultimate owner of the assets;
- respect provisions that can guarantee suitable transfer pricing for intergroup transactions with the purpose of allocating generated income in compliance with law;
- assist competent authorities in order to provide complete, truthful information necessary for tax obligations and controls;
- establish cooperative relations with the tax authorities, based on transparency and reciprocal trust and aimed at preventing conflict, limiting disputes as far as possible;
- propose products and services to customers that do not make it possible to unduly have tax benefits that could not otherwise be obtained, through adopting appropriate safeguards to avoid involvement in improper tax transactions of customers.

In any case, it is forbidden to engage/collaborate in or induce conduct which may belong to one of the types of offence covered by Legislative Decree No. 231/2001; more specifically, purely by way of example and without limitation it is forbidden to:

- provide incomplete documentation and/or communicate false or modified data;
- adopt deceitful conduct which might lead the Tax Authorities into error;

- pay an invoice without checking the actual existence, quality, suitability and prompt nature of the service received, and that the counterparty has met all obligations;
- use false structures or companies, not related to the business activity, solely for the purpose of tax evasion
- issue invoices or other documents for non-existent transactions in order to enable third parties to evade taxation;
- indicate in annual income tax and VAT returns: i) fictitious payable items, using invoices or other documents which are equivalent, in terms of evidence, to invoices, for non-existent transactions; ii) items receivable for an amount lower than the actual amount or fictitious payable items (for example costs fictitiously incurred and/or revenues indicated that are lower than the actual amount) referring to a false entry in mandatory accounting records and using means suitable for obstructing assessment; iii) a taxable base of a lower amount than the actual amount, by presenting items receivable for an amount lower than the actual amount or fictitious items payable; iv) apply, without reason, the terms of applicable legislation for presenting items, and for subsequent payment of resulting taxes.

The Heads of the Structures concerned are obliged to implement all measures necessary to guarantee the efficiency and actual implementation of the control and conduct principles described in this protocol.

8 APPENDIX: Bribery act

The Bribery Act entered into force in the United Kingdom on 1 July 2011. This Act modified and supplemented the pre-existing legislation governing corruption, introducing, inter alia, a new liability upon entities for cases of corruption in their favour or in their interest, where such entities do not have in place adequate internal procedures to prevent said offences.

More specifically, British law set forth a homogeneous set of regulations governing corruption, based on four main types of offence:

- the first relates to the offer, the promise or the grant to others of financial or other type of advantage in order to obtain or compensate the illegal execution of activities or services falling within their purview of control or responsibility or that of third parties (the purview of activities are defined in the law both in the public sector as well as for private professional and commercial activities);
- the second type consists in requesting, receiving or accepting to receive such advantage (an attempt is also punishable);
- the third case concerns the crime of "*Corruption of a foreign public official*", extending application of relevant provisions to outside the United Kingdom;
- the fourth hypothesis configures the "corporate offence", consisting of a commercial company's failure to adopt appropriate measures to prevent bribery episodes committed by the so-called "associated persons", meaning those persons who perform a service in the name of or on behalf of the company, irrespective of the nature of the relationship existing between the person and the company. In cases where the person is an employee, unless evidence to the contrary is given, the person is presumed to be an associated person.

With particular reference to the last type of offence (Failure of commercial organizations to prevent bribery) it must be pointed out as follows:

- bodies which do not carry out activities which fall under "business" are excluded;
- only the conduct of the "associated person" is taken into consideration for the existence of the liability of the entity;
- the liability of the entity exists only if the associated person is guilty of an offence in terms of the Bribery Act (corruption of a private individual or of a public official);
- the entity could be exempt from liability if it proves to have adopted, prior to the offence, "adequate procedures" aimed at preventing corruption.

The Bribery Act provides for the liability of entities that engage in such criminal conduct (so-called "corporate offence") unlimited fines, and for the perpetrators of the offence of bribery unlimited fines and imprisonment.

The Bribery Act is relevant to Italian companies insofar as it applies to all companies (whether British or not) which exercise their activities or part thereof in the United Kingdom.

Therefore, the Company Structures, as well as all employees and those who carry out a service in the name and on behalf of the Bank and who work with British counterparts or, in any event, in the United Kingdom, besides respect for the provisions of the Code of Ethics, the Group Internal Code of Conduct, the Group Anti-corruption Guidelines and this "Organisational, management and control model pursuant to Legislative Decree No. 231 of 8 June 2001", must also abide by the provisions of the Bribery Act and pro tempore internal regulations applicable to the London Branch in this respect (particularly the ISP London Anti-Bribery & Corruption policy available at the Company document repository).