MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL DECRETO LEGISLATIVO N. 231 DELL'8 GIUGNO 2001 E SUCCESSIVE MODIFICHE

INDICE

1. CONTESTO NORMATIVO

In attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 (di seguito denominato il "Decreto" o anche "D.Lgs. n. 231/2001"), con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche.

Il Decreto, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa a carico degli enti (da intendersi come società, associazioni, consorzi, ecc., di seguito denominati "Enti") per reati tassativamente elencati e commessi nel loro interesse o vantaggio: (i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi, ovvero (ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

Il catalogo dei "reati presupposto" si è dilatato nel tempo con l'introduzione anche di alcune fattispecie di illecito amministrativo.

La responsabilità dell'Ente si aggiunge a quella della persona fisica, che ha commesso materialmente l'illecito, ed è autonoma rispetto ad essa, sussistendo anche quando l'autore del reato non è stato identificato, o non è imputabile, oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti ivi espressamente previsti, gli Enti che abbiano tratto vantaggio dalla commissione del reato o nel cui interesse siano stati compiuti i reati presupposto – o gli illeciti amministrativi – di cui al Decreto medesimo. A carico dell'Ente sono irrogabili sanzioni pecuniarie e interdittive, nonché la confisca, la pubblicazione della sentenza di condanna ed il commissariamento. Le misure interdittive, che possono comportare per l'Ente conseguenze più gravose rispetto alle sanzioni pecuniarie, consistono nella sospensione o revoca di licenze e concessioni, nel divieto di contrarre con la Pubblica Amministrazione, nell'interdizione dall'esercizio dell'attività, nell'esclusione o revoca di finanziamenti e contributi, nel divieto di pubblicizzare beni e servizi. La suddetta responsabilità si configura anche in

relazione a reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'Ente abbia nel territorio dello Stato italiano la sede principale.

Istituita la responsabilità amministrativa degli Enti, l'art. 6 del Decreto stabilisce che l'Ente non risponde nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, "modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi". La medesima norma prevede, inoltre, l'istituzione di un "organismo di controllo interno all'Ente", con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza dei predetti modelli, nonché di curarne l'aggiornamento.

Il modello di organizzazione, gestione e controllo (di seguito "Modello", o "Modello di organizzazione, gestione e controllo") deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Ove il reato venga commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente, o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che:

i. il Consiglio di Amministrazione ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;
ii. il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento è stato affidato a un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo;
iii. i soggetti hanno commesso il reato eludendo fraudolentemente il Modello;

iv. non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi, secondo una valutazione che deve necessariamente essere effettuata a priori.

2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI KAIROS PARTNERS SGR S.P.A.

2.1. STRUMENTI DEL MODELLO

Nella predisposizione del presente Modello si è tenuto innanzitutto conto della normativa, delle procedure e dei sistemi di controllo esistenti e già operanti in Kairos Partners SGR S.p.A., in quanto idonei a valere anche come misure di prevenzione di reati e di comportamenti illeciti in genere, inclusi quelli previsti dal D.Lgs. n. 231/2001.

Kairos Partners SGR S.p.A. (di seguito denominata anche la "SGR" o la "Società") rappresenta una realtà complessa, sia sotto il profilo organizzativo che operativo. Gli organi della SGR hanno dedicato e continuano a dedicare la massima cura nella definizione della struttura organizzativa e delle procedure operative, sia al fine di assicurare efficienza, efficacia e trasparenza nella gestione delle attività e nell'attribuzione delle relative responsabilità, sia allo scopo di ridurre al minimo disfunzioni, malfunzionamenti ed irregolarità (tra i quali si annoverano anche comportamenti illeciti o comunque non in linea con quanto indicato dalla SGR).

Il contesto organizzativo nel quale Kairos Partners SGR S.p.A. opera è costituito dall'insieme di regole e procedure che garantiscono il funzionamento della Società; si tratta di un sistema estremamente articolato che viene definito e verificato internamente anche al fine di rispettare le previsioni normative a cui Kairos Partners SGR S.p.A. è sottoposta in qualità di società di gestione del risparmio. In tale sua qualità, la SGR è sottoposta alla vigilanza di Banca d'Italia e di Consob, ognuna per i profili di rispettiva competenza, le quali svolgono verifiche e controlli sull'operato della SGR e su aspetti relativi alla sua struttura organizzativa, come previsto dalla normativa.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli sull'attività di impresa, anche in relazione ai reati e agli illeciti da prevenire, la SGR ha individuato ed approvato:

- regolamenti interni, procedure e policy aziendali;
- un Codice Etico e un Regolamento sulle operazioni personali;
- il sistema dei controlli interni;
- il sistema delle deleghe e dei poteri.

Nei paragrafi che seguono si intendono illustrare, per grandi linee, i principi del Codice Etico e del Regolamento sulle operazioni personali, il sistema dei controlli interni, nonché il sistema dei poteri e delle deleghe.

2.1.1. CODICE ETICO E REGOLAMENTO SULLE OPERAZIONI PERSONALI

A conferma dell'importanza attribuita ai profili etici ed a coerenti comportamenti improntati a rigore e integrità, la SGR ha adottato un Codice Etico e un Regolamento sulle operazioni personali che rendono espliciti i fondamenti della propria cultura aziendale e i valori di riferimento dai quali la Società stessa fa derivare regole concrete di comportamento verso tutti i soggetti interni ed esterni, che hanno direttamente o indirettamente una relazione con la SGR. Il Codice Etico e il Regolamento sulle operazioni personali contengono rispettivamente un insieme di regole di carattere generale (che definiscono le norme essenziali di comportamento degli esponenti aziendali, dei dipendenti e dei collaboratori che, nell'ambito delle loro funzioni, sono tenuti ad esercitare le proprie attività con professionalità, diligenza, onestà e correttezza), e uno di carattere più specifico, ad esempio laddove si sottopongano ad autorizzazione preventiva determinate operazioni personali.

2.1.2. SISTEMA DEI CONTROLLI INTERNI

Kairos Partners SGR S.p.A., per garantire una sana e prudente gestione, coniuga la profittabilità dell'impresa con un'assunzione dei rischi consapevole e con una condotta operativa improntata a criteri di correttezza. Pertanto, la SGR, in linea con la normativa di legge e di vigilanza, si è dotata di un sistema dei controlli interni idoneo a rilevare, misurare e verificare nel continuo i rischi tipici dell'attività sociale. Il sistema dei controlli interni della SGR è insito nell'insieme di regole e procedure che mirano ad assicurare il rispetto delle strategie aziendali e il conseguimento delle seguenti finalità:

- efficacia ed efficienza dei processi aziendali;
- salvaguardia del valore delle attività e protezione dalle perdite;
- affidabilità e integrità delle informazioni contabili e gestionali;
- conformità delle operazioni con la legge, la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne.

Il sistema dei controlli interni è delineato da un'infrastruttura documentale (impianto normativo) che permette di ripercorrere in modo organico e codificato le linee guida, le procedure, i rischi ed i controlli presenti in azienda, recependo, oltre agli indirizzi aziendali e alle indicazioni degli Organi di Vigilanza,

anche le disposizioni di legge, ivi compresi i principi dettati dal D.Lgs. n. 231/2001. L'impianto normativo è costituito da documenti di governance, tempo per tempo adottati, che sovraintendono al funzionamento della SGR (statuto, Codice Etico eRegolamento sulle operazioni personali, Regolamento dei Comitati degli Investimenti, Regolamento delle funzioni di controllo, policy, funzionigramma, ecc.) e da norme più strettamente operative che regolamentano i processi aziendali, le singole attività e i relativi controlli (Procedure interne, Manuali, ecc.).

Più nello specifico le regole aziendali disegnano soluzioni organizzative che:

- assicurano una sufficiente separatezza tra le funzioni operative e quelle di controllo ed evitano situazioni di conflitto di interesse nell'assegnazione delle competenze;
- sono in grado di identificare, misurare e monitorare adeguatamente i principali rischi assunti nei diversi segmenti operativi;
- consentono la registrazione di ogni fatto di gestione e, in particolare, di ogni operazione con adeguato grado di dettaglio, assicurandone la corretta attribuzione sotto il profilo temporale;
- assicurano sistemi informativi affidabili e idonee procedure di reporting ai diversi livelli direzionali ai quali sono attribuite funzioni di controllo;
- garantiscono che le anomalie riscontrate dalle unità operative e dalle funzioni di controllo siano tempestivamente portate a conoscenza di livelli appropriati dell'azienda e gestite con immediatezza.

Inoltre, le soluzioni organizzative aziendali prevedono attività di controllo a ogni livello operativo che consentono l'univoca e formalizzata individuazione delle responsabilità, in particolare nei compiti di controllo e di correzione delle irregolarità riscontrate. La SGR, in coerenza con le indicazioni degli Organi di Vigilanza, ha individuato le seguenti macro tipologie di controllo:

- controlli di linea, diretti ad assicurare il corretto svolgimento dell'operatività quotidiana e delle singole transazioni. Di norma tali controlli sono effettuati dalle strutture operative, o incorporati nelle procedure informatiche, ovvero eseguiti nell'ambito dell'attività di back-office;
- controlli sulla gestione dei rischi, che hanno l'obiettivo di concorrere alla definizione delle metodologie di misurazione del rischio, verificare il rispetto dei limiti assegnati alle varie funzioni operative e controllare la coerenza dell'operatività delle singole strutture produttive con gli obiettivi di rischio rendimento assegnati. Essi sono affidati di norma a strutture diverse da quelle produttive;

- controlli di conformità, costituiti da politiche e procedure in grado di individuare, valutare, controllare e gestire il rischio conseguente al mancato rispetto di leggi, provvedimenti delle Autorità di Vigilanza e norme di autoregolamentazione, nonché ad ogni altra norma applicabile alla SGR;
- controlli di revisione interna, volti ad individuare andamenti anomali, violazioni delle procedure e della regolamentazione, nonché a valutare la funzionalità del complessivo sistema dei controlli interni. Tali controlli sono svolti da strutture indipendenti da quelle produttive.

Il sistema dei controlli interni è periodicamente soggetto a ricognizione e adeguamento in relazione all'evoluzione dell'operatività aziendale e al contesto di riferimento.

2.1.3. SISTEMA DELLE DELEGHE E DEI POTERI

Il Consiglio di Amministrazione è investito di tutti i poteri per l'ordinaria e straordinaria amministrazione della SGR e ha delegato alcune delle proprie attribuzioni all'Amministratore Delegato, determinandone i relativi poteri. Il Consiglio di Amministrazione ha inoltre definito l'ambito dei poteri deliberativi e di spesa conferiti ai Responsabili delle direzioni\unità organizzative, in coerenza con le responsabilità organizzative e gestionali attribuite, predeterminandone i limiti. Sono inoltre formalizzati le modalità di firma sociale per atti, contratti, documenti e corrispondenza, e i poteri attribuiti ai dipendenti. Tutte le direzioni\unità organizzative operano sulla base del funzionigramma aziendale e delle procedure interne, che definiscono i rispettivi ambiti di competenza e di responsabilità; il funzionigramma aziendale e le procedure interne sono diffuse in modo capillare all'interno della SGR. Pertanto i principali processi decisionali ed attuativi riguardanti l'operatività della SGR sono codificati, monitorabili e conoscibili da tutta la struttura.

2.2. FINALITÀ DEL MODELLO

Nonostante gli strumenti aziendali illustrati nei paragrafi precedenti risultino di per sé idonei anche a prevenire i reati contemplati dal Decreto, la SGR ha ritenuto opportuno adottare uno specifico Modello di organizzazione, gestione e controllo ai sensi del Decreto, nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione per tutti coloro che operano per conto della SGR, affinché tengano comportamenti corretti e lineari, anche un più efficace mezzo di prevenzione contro il rischio di commissione dei reati e degli illeciti amministrativi previsti dalla normativa di riferimento.

In particolare, attraverso l'adozione ed il costante aggiornamento del Modello, la SGR si propone di perseguire le seguenti principali finalità:

- determinare, in tutti coloro che svolgono per conto della SGR attività nel cui ambito è più verosimile il rischio della commissione dei reati presupposto previsti dal Decreto (attività "sensibili", nel seguito), la consapevolezza di poter incorrere, in caso di violazione delle disposizioni impartite in materia, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative irrogabili nei loro stessi confronti;
- ribadire che tali forme di comportamento illecito sono fortemente condannate, in quanto le stesse (anche nel caso in cui la SGR fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la SGR intende attenersi nell'esercizio dell'attività aziendale;
- consentire alla SGR, grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello.

2.3. ELEMENTI DEL MODELLO

Gli elementi fondamentali sviluppati nella definizione del Modello possono essere così riassunti:

- individuazione delle aree di attività a rischio, ovvero delle attività aziendali "sensibili" nel cui ambito potrebbero configurarsi le ipotesi di reato da sottoporre ad analisi e monitoraggio;
- gestione di processi operativi che garantiscano la separazione dei compiti, una chiara e formalizzata assegnazione dei poteri e delle responsabilità e la gestione dei processi decisionali;
- tracciabilità degli atti e tracciabilità ed esistenza delle attività di controllo e supervisione;
- emanazione di regole comportamentali idonee a garantire l'esercizio delle attività nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale;
- definizione delle responsabilità nell'adozione, modifica, attuazione e controllo del Modello stesso;
- identificazione di un "organismo di vigilanza" ("Organismo di Vigilanza", nel seguito) e attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- definizione di flussi informativi nei confronti dell'Organismo di Vigilanza;
- definizione e applicazione di disposizioni idonee a sanzionare il mancato rispetto delle misure indicate nel Modello;
- formazione del personale e comunicazione interna in merito al contenuto del Decreto e del

Modello ed agli obblighi che ne conseguono.

2.4. STRUTTURA DEL MODELLO

Nel definire il presente Modello di organizzazione, gestione e controllo, Kairos Partners SGR S.p.A. ha adottato un approccio che le ha consentito di utilizzare le regole e la normativa interna esistenti, integrandole nel Modello stesso.
Sono state così identificate, per ciascuna categoria di "reati presupposto", le attività "sensibili", ovvero, le attività aziendali nello svolgimento delle quali è più verosimile il rischio della commissione dei reati presupposto previsti dal Decreto, codificando per ciascuna di dette attività principi di comportamento e di controllo - diversificati in relazione allo specifico rischio/ reato da prevenire - cui devono attenersi tutti coloro che vi operano.

L'approccio seguito:

- consente di valorizzare al meglio il patrimonio conoscitivo già esistente in azienda in termini di politiche, regole e normative interne che indirizzano e governano la formazione e l'attuazione delle decisioni della SGR in relazione agli illeciti da prevenire e, più in generale, la gestione dei rischi e l'effettuazione dei controlli;
- permette di gestire con criteri univoci le regole operative aziendali, incluse quelle relative alle aree "sensibili";
- rende più agevole la costante implementazione e l'adeguamento tempestivo dei processi e dell'impianto normativo interni ai mutamenti della struttura organizzativa e dell'operatività aziendale, assicurando un elevato grado di "dinamicità" del Modello.

In Kairos Partners SGR S.p.A. il presidio dei rischi rivenienti dal D.Lgs. n. 231/2001 è pertanto assicurato:

- dal presente documento;
- dall'impianto normativo esistente, che ne costituisce parte integrante e sostanziale;
- dal Risk Assessment, nella parte in cui (considerata la sua natura di documento sempre in progress e la sua funzione) individua nel dettaglio le singole attività a rischio reato e i connessi presidi aziendali. Ciò significa che il Modello è necessariamente integrato dal Risk Assessment in relazione sia alla puntuale individuazione delle attività a rischio reato, all'interno dei processi aziendali, sia all'individuazione dei protocolli 231 ad essi associati, ove coincidenti con policy aziendali vigenti

espressamente richiamate dal Risk Assessment.

Il Modello di organizzazione, gestione e controllo delinea in particolare:

- il contesto normativo di riferimento;
- il ruolo e la responsabilità delle strutture coinvolte nell'adozione, efficace attuazione e aggiornamento del Modello;
- gli specifici compiti e responsabilità dell'Organismo di Vigilanza;
- i flussi informativi verso l'Organismo di Vigilanza;
- il sistema sanzionatorio;
- le logiche formative;
- le aree "sensibili" in relazione alle fattispecie di illecito di cui al Decreto;
- le attività aziendali nell'ambito delle quali può verificarsi il rischio di commissione dei reati presupposto, i principi di comportamento e le regole di controllo volti a prevenirli (attività "sensibili").

L'impianto normativo della SGR, costituito dai documenti di governance citati e contenuto in un'apposita sezione della intranet di Compliance, regolamenta ai vari livelli l'operatività della SGR nelle aree/attività "sensibili" e costituisce a tutti gli effetti parte integrante del Modello.

2.5. DESTINATARI DEL MODELLO

Il Modello, e le disposizioni ivi contenute e richiamate, devono essere rispettati dagli esponenti aziendali, da tutto il personale della SGR e, in particolare, da coloro che si trovino a svolgere le attività "sensibili".

La formazione del personale e l'informazione interna sul contenuto del Modello vengono costantemente assicurati con le modalità in seguito descritte.

Al fine di garantire l'efficace ed effettiva prevenzione dei reati, il Modello è destinato anche ai soggetti esterni (intendendosi per tali i lavoratori autonomi, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) che, in forza di rapporti contrattuali, prestino la loro collaborazione alla SGR per la realizzazione delle sue attività.

2.6. ADOZIONE, ATTUAZIONE E MODIFICHE DEL MODELLO

L'adozione e l'efficace attuazione del Modello costituiscono, ai sensi dell'art. 6, comma 1, lett. a) del Decreto, atti di competenza e di emanazione del Consiglio di Amministrazione che approva, mediante apposita delibera, il Modello, su proposta dell'Amministratore Delegato.

L'Amministratore Delegato definisce la struttura del Modello da sottoporre all'approvazione del Consiglio di Amministrazione con il supporto, per gli ambiti di rispettiva competenza, dell'Unità Compliance, dell'Unità Internal Audit e dell'Unità Affari Legali e Societari, e sentito il parere dell'Organismo di Vigilanza.

È cura del Consiglio di Amministrazione provvedere all'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'Organo amministrativo si avvale del supporto dell'Organismo di Vigilanza.

L'Organismo di Vigilanza conserva, in ogni caso, compiti e poteri in merito alla cura, sviluppo e promozione del costante aggiornamento del Modello. A tal fine può formulare osservazioni e proposte, attinenti l'organizzazione ed il sistema di controllo, alle unità organizzative a ciò preposte ovvero, in casi di particolare rilevanza, direttamente al Consiglio di Amministrazione. L'Organismo di Vigilanza provvede, senza indugio, a rendere operative le modifiche del Modello deliberate dal Consiglio di Amministrazione ed a curare la divulgazione dei contenuti all'interno della SGR e, per quanto necessario, anche all'esterno della stessa.

L'Organismo di Vigilanza provvede, altresì, mediante apposita relazione[1], ad informare il Consiglio di Amministrazione, con cadenza annuale, circa le attività di aggiornamento e/o adeguamento del Modello.

Per garantire che le variazioni del Modello siano operate con la necessaria tempestività e snellezza, anche al fine di ridurre al minimo i disallineamenti tra i processi operativi, da un lato, e le prescrizioni contenute nel Modello e la diffusione delle stesse, dall'altro, il Consiglio di Amministrazione ha ritenuto di delegare all'Organismo di Vigilanza il compito di apportare, con cadenza periodica, le

[1] Trattasi della relazione riepilogativa dell'attività svolta nell'anno, contenente anche un piano delle attività previste per l'anno successivo, presentata al Consiglio di Amministrazione e redatta dall'Organismo di Vigilanza entro 90 giorni dalla fine dell'esercizio sociale.

eventuali modifiche del Modello che attengono ad aspetti di carattere puramente descrittivo.

Sono aspetti di carattere puramente descrittivo quelli che attengono al recepimento nel Modello di deliberazioni assunte dal Consiglio di Amministrazione in materie non riguardanti direttamente il Modello, ovvero da soggetti delegati (es. variazioni/introduzione processi e procedure, emissione nuova normativa, etc.).

3. ORGANISMO DI VIGILANZA

3.1. INDIVIDUAZIONE DELL'ORGANISMO DI VIGILANZA

Ai sensi del Decreto, il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello, nonché di curarne l'aggiornamento, deve essere affidato ad un organismo interno all'Ente dotato di autonomi poteri di iniziativa e di controllo: l'Organismo di Vigilanza.

Le attribuzioni ed i poteri dell'Organismo di Vigilanza (di seguito, anche "Organismo") sono conferiti ad un organo collegiale nominato dal Consiglio di Amministrazione e avente caratteristiche di autonomia, indipendenza, professionalità e continuità di azione necessarie per il corretto ed efficiente svolgimento delle funzioni ad esso assegnate. Dell'avvenuta nomina dell'Organismo è data formale comunicazione a tutti i livelli aziendali.

L'Organismo di Vigilanza è dotato di poteri di iniziativa e di controllo sulle attività della Società, senza disporre di poteri gestionali e/o amministrativi.

Inoltre, onde poter svolgere in assoluta indipendenza le proprie funzioni, esso dispone di autonomi poteri di spesa sulla base di un budget, approvato dal Consiglio di Amministrazione, su proposta dell'Organismo stesso.

Il funzionamento dell'Organismo di Vigilanza è disciplinato dal presente Modello.

L'Organismo di Vigilanza si avvale ordinariamente delle strutture della Società per l'espletamento dei propri compiti di vigilanza e controllo ed in primis delle funzioni di controllo. Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, può inoltre avvalersi di consulenti esterni.

L'Organismo di Vigilanza, direttamente o per il tramite delle varie unità organizzative aziendali all'uopo designate, ha accesso a tutte le attività svolte dalla Società e alla relativa documentazione.

3.2. COMPOSIZIONE, DURATA E COMPENSI DELL'ORGANISMO DI VIGILANZA

3.2.1. COMPOSIZIONE

Al fine di assicurare la massima indipendenza, l'Organismo di Vigilanza è composto da tre membri, di cui almeno uno indipendente, individuati come segue:

1. professionisti esterni in possesso di adeguate competenze specialistiche (quali meglio specificate infra), e/o Amministratori indipendenti e non operativi, e/o Sindaci effettivi;
2. il Responsabile dell'Unità Internal Audit, e/o il Responsabile dell'Unità Compliance, e/o il Responsabile dell'Unità Affari Legali e Societari della Società.

L'Organismo nomina al proprio interno il Presidente.

Al fine di assicurare l'operatività dell'Organismo di Vigilanza, anche nei casi di sospensione ovvero di temporaneo impedimento di uno dei suoi membri, il Consiglio di Amministrazione può nominare altresì un componente supplente.

Può essere nominato membro supplente:

- un Amministratore indipendente e non operativo;
- un Sindaco effettivo o supplente;
- il Responsabile dell'Unità Internal Audit;
- il Responsabile dell'Unità Affari Legali e Societari;
- il Responsabile dell'Unità Compliance.

Laddove il membro supplente sia chiamato a sostituire il cosiddetto componente esterno dell'Organismo, egli sarà scelto fra un Amministratore indipendente e non operativo, un Sindaco effettivo o un Sindaco supplente; laddove il membro supplente sia chiamato a sostituire il cosiddetto componente interno dell'Organismo, egli sarà scelto fra il Responsabile dell'Unità Internal Audit, il Responsabile dell'Unità Affari Legali e Societari, o il Responsabile dell'Unità Compliance della SGR.

3.2.2. DURATA

L'Organismo di Vigilanza resta in carica per la durata stabilita dal Consiglio di Amministrazione all'atto della nomina; in assenza di una specifica determinazione in tal senso, esso dura per tutto il periodo in

cui resta in carica il Consiglio di Amministrazione che lo ha nominato. La revoca dei componenti - fatti salvi i casi disciplinati nel presente Modello - può avvenire unicamente nel caso di rilevanti inadempimenti nell'assolvimento dei loro compiti.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o decadenza, la maggioranza dei componenti. In tal caso il Consiglio di Amministrazione provvede tempestivamente a nominare i nuovi membri.

3.2.3. COMPENSI

Il Consiglio di Amministrazione, con astensione di quei componenti che eventualmente rivestano la qualifica di membro dell'Organismo di Vigilanza, delibera il compenso spettante - per tutta la durata della carica - al Presidente dell'Organismo di Vigilanza, per lo svolgimento delle relative funzioni, e ai membri esterni.

Ai membri – effettivi e supplenti – compete altresì il rimborso delle spese vive e documentate sostenute per intervenire alle riunioni.

3.3. REQUISITI DI ELEGGIBILITÀ, CAUSE DI DECADENZA E SOSPENSIONE

3.3.1. REQUISITI

I componenti dell'Organismo di Vigilanza devono possedere requisiti di professionalità, onorabilità ed indipendenza.

Fermo restando il possesso dei requisiti disposti dalla disciplina legale e regolamentare applicabile alla Società per Amministratori e Sindaci, gli altri membri dell'Organismo dovranno possedere i requisiti di onorabilità previsti per gli esponenti aziendali delle società di gestione del risparmio.

In aggiunta a quanto sopra:

- l'Amministratore non deve essere destinatario di deleghe esecutive e deve possedere i requisiti di indipendenza di tempo in tempo vigenti; laddove nessuno degli Amministratori abbia entrambi i requisiti, viene nominato un Sindaco effettivo;
- il professionista esterno deve essere scelto tra esperti (quali, ad esempio, docenti o liberi professionisti) in materie giuridiche, economiche, finanziarie o tecnico-scientifiche, ovvero tra

magistrati in quiescenza, o comunque tra soggetti in possesso di competenze specialistiche adeguate alla funzione, derivanti, ad esempio, dall'aver svolto per un congruo periodo di tempo attività professionali in materie attinenti al settore nel quale la Società opera, e/o dall'avere una adeguata conoscenza dell'organizzazione e dei principali processi aziendali;

- il professionista esterno non deve essere uno "stretto familiare" degli esponenti o dei top manager della Società[2].

In aggiunta al possesso dei requisiti sopra richiamati, i membri effettivi e l'eventuale membro supplente dovranno essere in possesso dei seguenti ulteriori requisiti di onorabilità, secondo i quali non possono essere eletti componenti dell'Organismo di Vigilanza coloro i quali:

- siano stati condannati, con sentenza irrevocabile o con sentenza non definitiva anche se a pena condizionalmente sospesa, fatti salvi gli effetti della riabilitazione, per uno dei reati tra quelli per i quali è applicabile il D.Lgs. n. 231/2001. Per sentenza di condanna si intende anche quella pronunciata ai sensi dell'art. 444 c.p.p.;
- abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, anche con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- abbiano subito l'applicazione delle sanzioni amministrative accessorie previste dall'art. 187 quater del D.Lgs. n. 58/1998.

Il Consiglio di Amministrazione verifica, entro 30 giorni dalla nomina, la sussistenza, in capo ai propri componenti effettivi e agli eventuali membri supplenti, dei requisiti ulteriori a quelli previsti dalla disciplina legale e regolamentare, sulla base di una dichiarazione resa dai singoli interessati.

3.3.2. DECADENZA

I componenti effettivi e supplenti dell'Organismo di Vigilanza, successivamente alla loro nomina, decadono da tale carica, qualora:

- se Consigliere di Amministrazione (o Sindaco) della Società, incorrano nella revoca o decadenza

[2] Sono considerati "stretti familiari" i familiari che ci si attende possano influenzare il, o essere influenzati dal, soggetto interessato nei rapporti con la Società. Essi possono includere:
a) il coniuge non legalmente separato e il convivente;
b) i figli e le persone a carico del soggetto, del coniuge non legalmente separato o del convivente.

da tale carica, anche in conseguenza del venir meno dei requisiti di professionalità, onorabilità e indipendenza prescritti dalla legge o dallo Statuto;

- dopo la nomina, si accerti che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- siano stati condannati, con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.), anche se a pena sospesa condizionalmente ai sensi dell'art. 163 c.p., per uno dei reati tra quelli per i quali è applicabile il D.Lgs. n. 231/2001;
- subiscano l'applicazione in via definitiva delle sanzioni amministrative accessorie previste dall'art. 187 quater del D.Lgs. n.58/1998.

I componenti dell'Organismo di Vigilanza debbono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause sopra elencate di decadenza.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una causa di decadenza, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione al membro che ricopra la carica di Consigliere (o di Sindaco), convoca senza indugio il Consiglio di Amministrazione affinché proceda – nella prima riunione utile successiva all'avvenuta conoscenza – alla dichiarazione di decadenza dell'interessato, per il venire meno dei requisiti previsti, dalla carica di componente dell'Organismo di Vigilanza ed alla sua sostituzione.

Resta in ogni caso ferma la facoltà di ciascun membro dell'Organismo di Vigilanza di rassegnare le dimissioni. In tale caso verrà sostituito con le medesime modalità descritte nel paragrafo precedente.

3.3.3. SOSPENSIONE

Costituiscono cause di sospensione dalla funzione di componente dell'Organismo di Vigilanza quelle che, ai sensi della vigente normativa di legge e regolamentare, comportano la sospensione dalla carica di Consigliere di Amministrazione ovvero di Sindaco**,** nonché le ulteriori di seguito riportate:

- si accerti, dopo la nomina, che i componenti dell'Organismo di Vigilanza hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate,

con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;

- i componenti dell'Organismo di Vigilanza siano stati condannati con sentenza non definitiva, anche a pena sospesa condizionalmente ai sensi dell'art. 163 c.p. (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.), per uno dei reati tra quelli per i quali è applicabile il D.Lgs. n. 231/2001.

In tali casi il Consiglio di Amministrazione dispone la sospensione della qualifica di membro dell'Organismo di Vigilanza e la cooptazione ad interim dell'eventuale membro supplente.

I componenti dell'Organismo di Vigilanza devono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause di sospensione di cui sopra.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una delle cause di sospensione dinazi citate, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione al membro che ricopra la carica di Consigliere (o di Sindaco), convoca senza indugio il Consiglio di Amministrazione affinché provveda, nella prima utile riunione successiva, a dichiarare la sospensione del soggetto, nei cui confronti si è verificata una delle cause di cui sopra, dalla carica di componente dell'Organismo di Vigilanza. In tal caso subentra ad interim l'eventuale membro supplente.

Fatte salve diverse previsioni di legge e regolamentari, la sospensione non può durare oltre sei mesi, trascorsi i quali il Presidente del Consiglio di Amministrazione iscrive l'eventuale revoca fra le materie da trattare nella prima riunione utile del Consiglio successiva a tale termine. Il componente non revocato è reintegrato nel pieno delle funzioni.

Qualora la sospensione riguardi il Presidente dell'Organismo di Vigilanza, la presidenza è assunta, per tutta la durata della medesima, dal componente più anziano di nomina o, a parità di anzianità di nomina, dal componente più anziano di età.

3.4. TEMPORANEO IMPEDIMENTO DI UN COMPONENTE

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente effettivo dell'Organismo di Vigilanza di svolgere le proprie funzioni ovvero di svolgerle con la necessaria

indipendenza ed autonomia di giudizio, questi è tenuto a dichiarare la sussistenza del legittimo impedimento, e, qualora quest'ultimo sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva, astenendosi dal partecipare alle sedute dell'Organismo o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso.

A titolo esemplificativo, costituiscono cause di temporaneo impedimento:

- la circostanza che il componente sia destinatario di un provvedimento di rinvio a giudizio in relazione ad un reato presupposto;
- la circostanza che il componente l'Organismo apprenda dall'Autorità Amministrativa di essere sottoposto alla procedura di irrogazione di una sanzione amministrativa di cui all'art. 187 quater del D.Lgs. n. 58/1998;
- malattia o infortunio che si protraggano per oltre sei mesi ed impediscano di partecipare alle riunioni dell'Organismo di Vigilanza.

Nel caso di temporaneo impedimento, subentra automaticamente ed in via temporanea l'eventuale membro supplente, il quale cessa dalla carica quando viene meno la causa che ha determinato il suo subentro.

Resta salva la facoltà per il Consiglio di Amministrazione, quando l'impedimento si protragga per un periodo superiore a sei mesi, prorogabile di ulteriori sei mesi per non più di due volte, di addivenire alla revoca del componente per il quale si siano verificate le predette cause di impedimento ed alla sua sostituzione con altro componente effettivo.

Qualora la sospensione o il temporaneo impedimento riguardi il Presidente, la presidenza è assunta ad interim dal componente effettivo più anziano di nomina o, a parità di anzianità di nomina, dal più anziano d'età.

3.5. COMPITI E POTERI

All'Organismo di Vigilanza sono affidati i seguenti compiti e poteri:

- vigilare sul funzionamento e l'osservanza del Modello;
- verificare l'effettiva idoneità del Modello a prevenire la commissione dei reati richiamati dal D.Lgs. 231/01;

- analizzare la persistenza nel tempo dei requisiti di solidità e funzionalità del Modello;
- curare, sviluppare e promuovere il costante aggiornamento del Modello, suggerendo, ove necessario, all'Organo amministrativo le correzioni e gli adeguamenti dovuti;
- mantenere i rapporti e assicurare i flussi informativi di competenza verso il Consiglio di Amministrazione ed il Collegio Sindacale;
- acquisire informazioni e documentazione di ogni tipo, da ogni livello e settore della SGR (a titolo esemplificativo ma non esaustivo, e con differente frequenza, la Relazione annuale del Responsabile dell'Unità Compliance, la Relazione annuale del Responsabile dell'Unità Internal Audit, la Relazione annuale del Responsabile dell'Unità Risk Management, la Relazione annuale del Responsabile Antiriciclaggio, la Relazione annuale sui fornitori di servizi, le informative annuali predisposte per il Consiglio di Amministrazione inerenti la market abuse e i conflitti di interesse, le richieste di dati e notizie provenienti da Consob, le rihieste provenienti da Banca d'Italia, un report predisposto dall'Unità Rapporti con le AA.VV. da cui risultino gli eventuali incontri con Banca d'Italia e Consob, un report predisposto dal Responsabile Antiriciclaggio da cui risultino eventuali incontri con l'Unità di Informazione Finanziaria, un report predisposto dall'Unità Affari Legali e Societari da cui derivino le richieste provenienti dalla Guardia di Finanza e gli eventuali incontri con la stessa, un report predisposto dall'Unità Risk Management sulle segnalazioni prodotte dal sistema in materia di market abuse, un report predisposto dall'Unità Risk Management da cui risultino informazioni in merito alla compilazione dell'agenda degli incontri, il "Documento di identificazione e di valutazione dei rischi" (ex art. 28 del D. Lgs. 81/2008), la "Valutazione e gestione del rischio da stress lavoro-correlato", etc.);
- compiere verifiche ed ispezioni al fine di accertare eventuali violazioni del Modello;
- elaborare un piano delle attività previste, in coerenza con i principi contenuti nel Modello;
- assicurare l'attuazione del piano di attività previste;
- assicurare l'elaborazione della reportistica sulle risultanze degli interventi effettuati;
- assicurare il costante aggiornamento del sistema di identificazione, mappatura e classificazione delle aree di rischio ai fini dell'attività di vigilanza propria dell'Organismo;
- fermo restando quanto già previsto dal presente documento, definire e promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché della formazione del personale e della sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
- fornire chiarimenti in merito al significato e all'applicazione delle previsioni contenute nel Modello;
- predisporre un efficace sistema di comunicazione interna per consentire la trasmissione e la

raccolta di notizie rilevanti ai fini del D.Lgs. 231/01, garantendo la tutela e riservatezza del segnalante;

- formulare la previsione di spesa per lo svolgimento della propria attività da sottoporre all'approvazione del Consiglio di Amministrazione; eventuali spese straordinarie dovranno essere parimenti sottoposte alla preventiva approvazione del Consiglio di Amministrazione;
- promuovere l'attivazione di eventuali procedimenti disciplinari e/o sanzioni.

3.6. PERIODICITÀ DELLE RIUNIONI, VALIDITÀ DELLE DELIBERAZIONI E VERBALIZZAZIONE

L'Organismo si riunisce di norma con periodicità semestrale e, in ogni caso, ogniqualvolta sia ritenuto necessario e/o opportuno dal Presidente o da altro membro.

La riunione è convocata dal Presidente presso la sede sociale della SGR o altrove. L'Organismo può riunirsi anche in videoteleconferenza. In tal caso l'Organismo si intende riunito nel luogo in cui si trova il Presidente.

Per la validità delle deliberazioni è necessaria la presenza della maggioranza dei membri.

Le deliberazioni sono prese a maggioranza assoluta dei membri presenti alle riunioni. In caso di parità, il voto del Presidente prevale.

Tutte le riunioni constano di un verbale sottoscritto dal Presidente e dal segretario, scelto di volta in volta dallo stesso Presidente tra i membri dell'Organismo.

3.7. INFORMATIVA AGLI ORGANI AZIENDALI

L'Organismo di Vigilanza informa il Consiglio di Amministrazione in merito all'applicazione e all'attuazione del Modello, nonché all'emersione di eventuali aspetti critici e alla necessità di interventi modificativi.

A tal fine l'Organismo di Vigilanza predispone:

- entro novanta giorni dalla chiusura di ciascun esercizio sociale, una relazione riepilogativa dell'attività svolta nell'anno trascorso ed un piano delle attività previste per il nuovo anno, da

presentare al Consiglio di Amministrazione[3];

- immediatamente, una comunicazione, da presentare al Consiglio di Amministrazione, relativa al verificarsi di situazioni straordinarie (ad esempio violazioni dei principi contenuti nel Modello), in caso di segnalazioni ricevute o di altre fattispecie che rivestono carattere d'urgenza.

[3] La citata relazione sarà presentata anche all'Assemblea dei Soci della SGR, in occasione dell'approvazione del Bilancio di esercizio.

4. FLUSSI INFORMATIVI

L'Organismo di Vigilanza deve essere informato mediante apposite segnalazioni da parte dei Responsabili delle funzioni aziendali, degli altri dipendenti, degli organi societari e dei soggetti esterni (intendendosi per tali i lavoratori autonomi, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) in merito ad eventi che potrebbero ingenerare responsabilità della SGR ai sensi del Decreto.

Devono essere segnalate senza ritardo:

- le notizie relative alla commissione, o alla ragionevole convinzione di commissione, degli illeciti per i quali è applicabile il D.Lgs. n. 231/2001, compreso l'avvio di procedimento giudiziario a carico di dirigenti/dipendenti per reati previsti nel D.Lgs. n. 231/2001;
- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello.

Le segnalazioni possono essere fatte dai dipendenti direttamente all'Organismo di Vigilanza, ovvero per il tramite dell'Unità Internal Audit, alla quale la segnalazione potrà essere inoltrata tanto direttamente, quanto mediante il responsabile dell'unità organizzativa di appartenenza.

I soggetti esterni, ivi compresi i soggetti che svolgono attività in outsourcing per conto della SGR, inoltrano la segnalazione direttamente al Responsabile dell'Unità Internal Audit. L'Organismo di Vigilanza valuta le segnalazioni ricevute e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione, e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna. L'Organismo di Vigilanza prenderà in considerazione le segnalazioni, ancorché anonime, che presentino elementi fattuali.

La SGR garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti della SGR, o delle persone accusate erroneamente e/o in mala fede.

Oltre alle segnalazioni relative alle violazioni sopra descritte, devono obbligatoriamente ed immediatamente essere trasmesse all'Organismo:

- per il tramite dell'Unità Internal Audit, le informazioni concernenti:

- i rapporti predisposti dalle funzioni aziendali nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- i procedimenti disciplinari promossi o, nel caso in cui dette violazioni siano commesse da soggetti non dipendenti, le iniziative sanzionatorie assunte;

- per il tramite della Funzione Antiriciclaggio:

  - le segnalazioni di infrazioni in materia di contrasto del riciclaggio e del finanziamento del terrorismo inoltrate alle competenti Autorità ai sensi dell'art. 52 del D.Lgs. n. 231/2007, secondo modalità e tempistiche previste dalle disposizioni interne tempo per tempo vigenti;

- per il tramite dell'Unità Compliance:

  - i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra Autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti ai quali è applicabile il D.Lgs. n. 231/2001, qualora tali indagini coinvolgano la SGR, o suoi dipendenti, o organi societari, o comunque la responsabilità della SGR stessa;

- per il tramite dell'Unità Affari Legali e Societari:

  - i provvedimenti e/o notizie e/o incontri provenienti/avvenuti dalla/con la Guardia di Finanza, fatti comunque salvi gli obblighi di segreto imposti dalla legge.

Ciascuna unità organizzativa cui sia attribuito un determinato ruolo in una fase di un processo sensibile deve segnalare tempestivamente all'Organismo di Vigilanza eventuali propri comportamenti significativamente difformi da quelli descritti nel processo e le motivazioni che hanno reso necessario od opportuno tale scostamento. Attraverso apposita procedura informatica, è garantita la possibilità di segnalazioni in termini anonimi. L'Unità Internal Audit, in caso di eventi che potrebbero ingenerare gravi responsabilità della SGR ai sensi del D.Lgs. n. 231/2001, informa tempestivamente il Presidente dell'Organismo di Vigilanza e predispone specifica relazione che descriva nel dettaglio l'evento stesso, il rischio, il personale coinvolto, i provvedimenti disciplinari in corso e le soluzioni per limitare il ripetersi dell'evento.

5. SISTEMA SANZIONATORIO E CODICE DISCIPLINARE

L'efficacia del Modello è assicurata - oltre che dall'elaborazione di meccanismi di decisione e di controllo tali da eliminare o ridurre significativamente il rischio di commissione degli illeciti penali ed amministrativi per i quali è applicabile il D.Lgs. n. 231/2001 - dagli strumenti sanzionatori posti a presidio dell'osservanza delle condotte prescritte. I comportamenti dei dipendenti e dei soggetti esterni, così come in precedenza descritti, non conformi ai principi e alle regole di condotta prescritti nel presente Modello - ivi ricomprendendo il Codice Etico e il Regolamento sulle operazioni personali e le procedure e norme interne - costituiscono illecito contrattuale.

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D.Lgs. 231/01 indicano, quale condizione per un'efficace attuazione del Modello, l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

La definizione di un efficace sistema disciplinare costituisce, pertanto, un presupposto essenziale della valenza scriminante del Modello rispetto alla responsabilità amministrativa degli Enti.

A tal fine la Società ha predisposto un Codice Disicplinare ad hoc, contenuto nel Modello, applicabile a tutti i lavoratori subordinati dipendenti, introdotto con finalità di prevenzione e sanzione rispetto a condotte poste in essere in violazione di disposizioni e/o procedure interne.

Esso si aggiunge e non sostituisce le norme disciplinari contenute nei contratti collettivi applicati e elenca la normativa di autoregolamentazione interna, predisposta a garanzia del corretto svolgimento dell'attività aziendale, anche in base alle norme di legge e/o regolamentari applicate alla Società. Il Codice Disciplinare richiama infatti procedure, regolamenti e policy predisposti dalla SGR e le correlate sanzioni, in conformità alle previsioni di legge e di contratto collettivo ed è portato a conoscenza di tutti i suoi destinatari con le stesse modalità di diffusione previste per il Modello che lo contiene, e quindi mediante pubblicazione sulla intranet di Compliance.

Ogni eventuale violazione dei suddetti principi, misure e procedure, rappresenta, se accertata:

- nel caso di lavoratori (anche con qualifica dirigenziale), un inadempimento contrattuale in relazione alle obbligazioni che derivano dal rapporto di lavoro ai sensi dell'art. 2104 cod. civ., con conseguente applicazione dell'art. 2106 cod. civ. e delle sanzioni previste dal Codice Disciplinare;
- nel caso di amministratori, l'inosservanza dei doveri ad essi imposti dalla legge e dallo statuto ai

sensi dell'art. 2392 cod. civ.;

- nel caso di soggetti non aventi un rapporto di lavoro subordinato con la SGR e non facenti parte dell'organo di amministrazione e/o di controllo (i "Soggetti Esterni"), costituisce inadempimento contrattuale e potrebbe legittimare la risoluzione del contratto, fatto salvo il risarcimento del danno.

Le sanzioni previste dal presente sistema disciplinare e dal correlato Codice Disciplinare qui riportato saranno applicate ad ogni violazione accertata delle disposizioni contenute nel Modello, a prescindere dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'Autorità Giudiziaria nel caso in cui il comportamento da censurare integri gli estremi di una fattispecie di reato rilevante ai sensi del D.Lgs. 231/01.

Ad ogni segnalazione di violazione del Modello proveniente dall'Organismo di Vigilanza, verrà promossa un'azione disciplinare, da parte dell'unità della SGR che assolve alla funzione di gestione delle risorse umane, finalizzata all'accertamento della responsabilità della violazione stessa. In particolare, nella fase di accertamento verrà previamente contestato al dipendente l'addebito e gli sarà, altresì, garantito un congruo termine per presentare le sue difese e giustificazioni alla contestazione. Una volta accertata tale responsabilità, sarà irrogata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa, nei termini meglio specificati ai sensi del Codice Disciplinare.

Ciascun dipendente è tenuto al rispetto degli obblighi derivanti dall'applicazione della seguente regolamentazione interna, oltre che al rispetto di ogni altra procedura/policy/regolamento interno espressamente richiamato nel Modello e nel Risk Assessment, nonché – in generale – del contratto collettivo applicabile al rapporto di lavoro e dalle norme di legge (artt. 2104, 2105 e 2106 del cod. civ.):

- Manuale delle Procedure – Aspetti di carattere generale;
- Regolamento del Comitato Remunerazioni;
- Regolamento del Comitato Rischi;
- Regolamento del Comitato Nomine;
- Regolamento del Comitato di Direzione;
- Regolamento del Comitato degli Investimenti;
- Regolamento del Comitato di Consulenza;
- Regolamento del Comitato di pricing e valutazione del merito creditizio;

- Regolamento del Comitato Prodotti;
- Gestioni Patrimoniali;
- Gestioni Collettive;
- Consulenza;
- Ricezione e Trasmissione di Ordini;
- Best Execution;
- Market Abuse;
- Processo di valorizzazione;
- Criteri di valutazione degli strumenti finanziari;
- Valutazione del merito creditizio;
- Politica di impegno ed esercizio dei diritti inerenti agli strumenti finanziari degli OICVM gestiti;
- Policy ESG;
- Processo distributivo;
- Collocamento;
- Antiriciclaggio;
- Know your Distributor;
- Offerta in sede e fuori sede;
- Adeguatezza, prodotti complessi e target market;
- Rapporti dormienti;
- Riascolto telefonate registrate;
- Conoscenze e competenze del personale;
- Incentivi;
- Domiciliazione della corrispondenza;
- Codice di condotta in materia fiscale;
- Contabilità e bilancio;
- Budget a analisi degli scostamenti;
- Ciclo passivo;
- Adempimenti fiscali;
- Gestione amministrativa del personale;
- Gestione dell'attivo patrimoniale;
- Prezzi di trasferimento per transazioni infragruppo;
- Linee guida per la revisione;

- Progetti Strategici;
- Product Governance;
- Nuovi prodotti;
- Parti correlate;
- Business Continuity Management System;
- Estrenalizzazione delle funzioni aziendali;
- Formazione esterna;
- Remunerazione e incentivazione;
- Information Technology;
- Segreteria societaria;
- Controversie legali;
- Gestione corrispondenza e segnalazioni alle AA.VV;
- Gestione archivio documentale;
- FATCA e QI;
- CRS;
- Manuale Qualified Intermediary Agreement;
- Consulenti legali esterni;
- EMIR;
- Controlli di linea;
- Voluntary Disclosure – Memorandum Operativo;
- Protezione dei dati personali;
- Disciplinare Interno Privacy;
- Organigramma in ambito GDPR;
- Linee-guida per la compilazione del registro dei trattamenti;
- Metodologia della valutazione dei rischi;
- Gestione responsabili esterni;
- Gestione del consenso;
- Gestione sistema videosorveglianza;
- Gestione trasferimento dati all'estero;
- Gestione accesso e manutenzone dei dati dell'interessato;
- Gestione informative;
- Gestione incidenti (data breach);

- Gestione revoca consenso;
- Gestione comunicazione interessati in caso di data breach;
- Gestione formazione;
- Attività di marketing relativa a soggetti non clienti.

Ciascun dipendente è altresì tenuto al rispetto degli obblighi derivanti dall'applicazione delle seguenti regole di condotta, nonché – in generale – dal contratto collettivo applicabile al rapporto di lavoro e dalle norme di legge (artt. 2104, 2105 e 2106 del cod. civ.):

- Codice Etico;
- Regolamento operazioni personali;
- Conflitti di interesse;
- Gift e Entertainment;
- Mandati e occupazioni secondarie;
- Spese di viaggio e trasferta;
- Utilizzo della firma sociale;
- Clear Desk Policy;
- Whistleblowing;
- Regolamento Covid-19.

Ciascun dipendente è tenuto infine al rispetto degli obblighi derivanti dall'applicazione di quanto contenuto nella seguente documentazione inerente talune unità organizzative, fra cui le funzioni di controllo, nonché – in generale – di quanto contenuto nel contratto collettivo applicabile al rapporto di lavoro e alle norme di legge (artt. 2104, 2105 e 2106 del cod. civ.):

- Affari Legali e Societari;
- Organizzazione;
- Rapporti con le AA.VV.;
- Regolamento Compliance;
- Trattazione dei reclami;
- Regolamento Risk Management;
- Manuale operativo Risk Management;
- Liquidity Stress Test;
- Mappatura rischi aziendali;

- Misure contro frodi ed attività improprie;
- Regolamento Internal Audit.

Le sanzioni irrogabili nei confronti dei lavoratori dipendenti della SGR, conformemente a quanto previsto dall'articolo 7 della Legge 20 maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) e dal contratto collettivo applicato, consistono in:

a) rimprovero verbale;
b) rimprovero scritto;
c) sospensione dal servizio e dal trattamento economico per un periodo non superiore a dieci giorni;
d) licenziamento per notevole inadempimento degli obblighi contrattuali del prestatore di lavoro (giustificato motivo);
e) licenziamento per mancanza così grave da non consentire la prosecuzione anche provvisoria del rapporto (giusta causa).

Le sanzioni di cui alle lettere a), b) e c) che precedono saranno adottate in caso di infrazioni che, in considerazione delle circostanze specifiche che le hanno determinate, non siano così gravi da rendere applicabile una diversa sanzione.

Le sanzioni di cui alle lettere d) ed e) saranno adottate nei confronti di dipendenti colpevoli di mancanze che siano così gravi da non consentire la prosecuzione del rapporto, oppure in caso di recidiva, oppure qualora la finalità della condotta sia quella di assicurare un vantaggio personale o della Società indipendentemente dalla gravità dell'inadempimento.

L'applicazione della sanzione prescinde dall'assenza di un eventuale danno economico subito dalla Società per effetto del comportamento tenuto in violazione della procedura.

L'applicazione della sanzione disciplinare prescinde altresì dall'instaurazione o meno dell'esito di un eventuale procedimento amministrativo e/o penale a carico del soggetto interessato, e fa in ogni caso salvo il diritto della Società di chiedere il risarcimento del danno.

Fermo quanto precede, la violazione delle procedure, dei regolamenti e delle policy assumerà rilevanza, oltre che sotto il profilo disciplinare, quale inadempimento degli obblighi derivanti dal rapporto contrattuale e/o organico intercorrente con la Società.

A seconda della gravità della violazione accertata, l'Organismo di Vigilanza suggerisce al datore di lavoro la sanzione che reputa più opportuna per la fattispecie occorsa.

Nella valutazione della gravità della violazione viene considerata:

- la tipologia;
- le circostanze;
- le modalità di commissione;
- l'elemento soggettivo;
- la funzione, il ruolo e le responsabilità dell'agente nell'ambito dell'organizzazione aziendale;
- le eventuali conseguenze derivanti dalla violazione, con particolare riferimento al rapporto fiduciario con la Società.

Nella determinazione della concreta sanzione da applicare sono inoltre considerati:

- la gravità della violazione;
- l'eventuale recidiva dell'agente.

Quando sia richiesto dalla natura della mancanza o dalla necessità di accertamenti in conseguenza della medesima, la Società – in attesa di deliberare l'eventuale definitivo provvedimento disciplinare – può disporre la sospensione temporanea del lavoratore dal servizio per il tempo strettamente necessario, ovvero - in via provvisoria e cautelare, per un periodo non superiore a tre mesi - l'adibizione del lavoratore ad incarichi diversi, nel rispetto di quanto disposto dall'art. 2103 c.c.

È inteso che saranno seguite tutte le disposizioni e le garanzie previste dalla legge e dai contratti di lavoro in materia di procedimento disciplinare; in particolare si rispetterà:

- l'obbligo - in relazione all'applicazione di qualunque provvedimento disciplinare - della previa contestazione dell'addebito al dipendente e dell'ascolto di quest'ultimo in ordine alla sua difesa;
- l'obbligo - salvo che per l'ammonizione verbale - che la contestazione sia fatta per iscritto e che il provvedimento non sia emanato se non decorsi i giorni, specificatamente indicati per ciascuna sanzione nei contratti di lavoro, dalla contestazione dell'addebito.

Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento e definizione dell'eventuale azione penale, in quanto i principi e le regole di condotta imposti dal Modello sono assunti dalla SGR in piena autonomia ed indipendentemente dai possibili reati che eventuali condotte

possano determinare e che l'Autorità Giudiziaria ha il compito di accertare.

La verifica dell'adeguatezza del sistema sanzionatorio nonché del Codice Disicplinare contenuto nel Modello, e il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, sono affidati all'Organismo di Vigilanza, il quale procede anche alla segnalazione delle infrazioni di cui venisse a conoscenza nello svolgimento delle funzioni che gli sono proprie.

Fermo restando quanto precede in merito alla generalità dei lavoratori dipendenti, si osserva che il rapporto di lavoro dirigenziale si caratterizza per la sua natura fiduciaria. Il comportamento del dirigente si riflette infatti non solo all'interno della Società, ma anche all'esterno; ad esempio in termini di immagine rispetto al mercato e in generale rispetto ai diversi portatori di interesse.

Pertanto, il rispetto da parte dei dirigenti della Società di quanto previsto nel presente Modello e l'obbligo di farlo rispettare è considerato elemento essenziale del rapporto di lavoro dirigenziale, poiché costituisce stimolo ed esempio per tutti coloro che da questi ultimi dipendono gerarchicamente.

Eventuali infrazioni poste in essere da dirigenti della Società, in virtù del particolare rapporto di fiducia esistente tra gli stessi e la Società potranno essere sanzionate con i provvedimenti disciplinari ritenuti più idonei al singolo caso. Ferma la facoltà di recesso, anche per giusta causa, le eventuali sanzioni saranno applicate nel rispetto dei principi generali precedentemente individuati.

In caso di violazione del Modello da parte di soggetti che ricoprono la funzione di componenti del Consiglio di Amministrazione della SGR, l'Organismo di Vigilanza informerà il Collegio Sindacale, il quale provvederà ad adottare le iniziative ritenute opportune in relazione alla fattispecie, nel rispetto della normativa vigente. Le sanzioni applicabili nei confronti degli amministratori sono la revoca delle deleghe o dell'incarico e, nel caso in cui l'amministratore sia legato alla Società da un rapporto di lavoro subordinato, il licenziamento.

Con riferimento ai Soggetti Esterni, la Società porterà a conoscenza degli stessi il contenuto e le disposizioni del Modello e del relativo sistema sanzionatorio, se del caso integrando gli attuali accordi contrattuali e richiedendo ai Soggetti Esterni l'accettazione delle relative previsioni, nonché il correlato obbligo di attenersi a quest'ultime.

L'Organismo di Vigilanza verifica che siano adottate procedure specifiche per trasmettere ai soggetti

esterni i principi e le linee di condotta contenute nel presente Modello e nei relativi regolamenti, protocolli e codici annessi.

Qualora sia accertata una violazione del modello da parte di un Soggetto Esterno, la Società applicherà una delle seguenti sanzioni:

- pagamento della penale contrattualmente stabilita, ove applicabile, salva la risarcibilità dell'eventuale maggior danno;
- risoluzione del contratto ai sensi dell'art. 1456 c.c. e pagamento della penale contrattualmente stabilita, salva la risarcibilità dell'eventuale maggior danno.

Nel caso in cui le violazioni del Modello siano commesse da lavoratori somministrati ovvero da prestatori di lavoro nell'ambito di contratti di appalto di opere o di servizi, ovvero da un lavoratore distaccato, la Società provvederà ad informare prontamente il somministrante o l'appaltatore o il distaccante per l'eventuale adozione, da parte di questi, dei provvedimenti sanzionatori nei confronti dei propri dipendenti e/o collaboratori.

Le violazioni del Modello commesse da dipendenti e/o collaboratori dei Soggetti Esterni saranno addebitate dalla Società a questi ultimi.

6. FORMAZIONE E INFORMAZIONE

Il regime della responsabilità amministrativa previsto dalla normativa di legge e l'adozione del Modello di organizzazione, gestione e controllo da parte della SGR formano un sistema che deve trovare nei comportamenti operativi del personale una coerente ed efficace risposta.

I neo assunti ricevono il link alla Intranet di Compliance[4], tramite la quale hanno a disposizione tutta la normativa di autoregolamentazione interna. Il Modello, le policy, il Manuale delle procedure e tutta la restante regolamentazione aziendale sono messe a disposizione nell'apposita sezione della citata Intranet sub "Aree Tematiche\Organismo di Vigilanza " per il Modello e le connesse Procedure ICT (reati informatici), sub "Aree Tematiche\Organizzazione" per Organigramma, Funzionigramma e Deleghe, sub "Aree Tematiche\Organi Aziendali" per il Regolamento del Consiglio di Amministrazione, il Regolamento del Collegio Sindacale, la Procedura di autovalutazione del Consiglio di Amministrazione e il Questionario di autovalutazione del Consiglio di Amministrazione, e, infine, sub "Aree Tematiche\Organizzazione\Policy e Procedure" per la restante normativa di autoregolamentazione. I neo assunti dovranno sottoscrivere un'apposita dichiarazione attestante la presa visione dei citati documenti e l'impegno ad osservare le relative prescrizioni all'atto dell'assunzione.

I documenti pubblicati sono costantemente aggiornati in relazione alle modifiche che via via intervengono nell'ambito della normativa di legge e del modello organizzativo.

In sintesi, l'insieme degli strumenti citati garantisce a tutto il personale una informazione completa e tempestiva.

Al fine di agevolare la comprensione del Modello, l'Organismo provvede, anche in collaborazione con altre funzioni aziendali, ad organizzare percorsi formativi per i dipendenti, che si potranno concretizzare nella distribuzione di prodotti di e-learning o in corsi da tenersi in aula.

L'Organismo provvederà nel corso di tali attività a rendere noto ai dipendenti che gli stessi sono tenuti a conoscere i principi ed i contenuti del Modello ed a contribuire, in relazione al ruolo ed alle responsabilità rivestite all'interno della SGR, alla sua attuazione ed al suo rispetto, segnalando

[4] In caso di modifiche ai citati documenti, l'informativa è resa tramite email da parte dell'Unità delegata dal Consiglio di Amministrazione.

eventuali carenze.

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

7. REATI PRESUPPOSTO

7.1. INDIVIDUAZIONE AREE SENSIBILI

L'art. 6, comma 2, del D.Lgs. n. 231/2001 prevede che il Modello debba "individuare le attività nel cui ambito possono essere commessi i reati".

Sono state pertanto analizzate le fattispecie dei "reati presupposto" per le quali si applica il Decreto; con riferimento a ciascuna categoria dei medesimi sono state identificate nella SGR le attività "sensibili" e le unità organizzative aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

Per ciascuna di tali attività "sensibili" si sono quindi qualificati i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

Sulla base delle disposizioni di legge attualmente in vigore, i "reati presupposto" individuati dal Modello riguardano:

- i reati contro la Pubblica Amministrazione di cui agli artt. 24 e 25 D.Lsg 231/01;
- i reati societari di cui all'art. 25-ter D.Lgs 231/01;
- i delitti di criminalità organizzata, con finalità di terrorismo (di cui all'art. 24-ter D.Lgs 231/01), di eversione dell'ordine democratico (di cui all'art. 25-quater D.Lgs 231/01) e i reati transazionali (di cui alla L. 146/2006);
- i delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria di cui all'art. 25-decise D.Lgs 231/01;
- i reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento di cui all'art. 25-bis D.Lgs;
- i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio di cui all'art. 25-octies;
- i reati ed illeciti amministrativi riconducibili ad abusi di mercato di cui all'art. 25-sexies D.Lgs 231/01;
- i reati in tema di salute e sicurezza sul lavoro di cui all'art. 25-septies D.Lgs 231/01;
- i delitti informatici e di trattamento illecito di dati (di cui all'art. 24-bis D.Lgs 231/01) e in materia di violazione del diritto d'autore (di cui all'art. 25-novies D.Lgs 231/01);

- delitti contro l'industria ed il commercio di cui all'art. 25-bis.1 D.Lgs 231/01;
- delitti contro la personalità individuale di cui all'art. 25-quinquies D.Lgs 231/01 e di impiego di cittadini di paesi terzi il cui soggiorno è irregolare di cui all'art. 25-duodecies D.Lgs 231/01;
- reati tributari di cui all'art. 25-quiquiesdecies D.Lgs 231/01.

Con riferimento ai sopra citati illeciti amministrativi, alcune singole fattispecie di reato presupposto sono emerse come non rilevanti per la Società; per questa ragione, nell'elenco dei reati presupposto che verrà offerto all'inizio di ciascuana Parte Speciale, verranno compresi solo quelli ritenuti rilevanti dal Risk Assessment.

Dal Risk Assessment, infine, è emersa la non rilevanza, in relazione ai processi aziendali della Società, dei seguenti illeciti amministrativi:

- Pratiche di mutilazione degli organi genitali femminali di cui all'art. 25-quater.1 D.Lgs 231/01;
- Reati ambientali di cui all'art. 25-undecies D.Lgs 231/01;
- Razzismo e xenofobia di cui all'art. 25-terdecies D.Lgs 231/01;
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati di cui all'art. 25-quaterdecies D.Lgs 231/01;
- Contrabbando di cui all'art. 25-sexiesdecies D.Lgs 231/01.

7.2. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Gli artt. 24 e 25 del Decreto contemplano una serie di reati previsti dal codice penale accomunati dall'identità del bene giuridico da essi tutelato, individuabile nell'imparzialità e nel buon andamento della Pubblica Amministrazione.

Agli effetti della legge penale si considera Ente della Pubblica Amministrazione qualsiasi persona giuridica che persegua e/o realizzi e gestisca interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, disciplinata da norme di diritto pubblico e manifestantesi mediante atti autoritativi.

A titolo meramente esemplificativo, ed avendo riguardo all'operatività della SGR, si possono individuare, esemplificativamente, quali soggetti appartenenti alla Pubblica Amministrazione:

- lo Stato, le Regioni, le Province, i Comuni;
- i Ministeri, i Dipartimenti, le Commissioni;
- gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT).

Le fattispecie penali qui considerate, nelle loro differenti tipicità, presuppongono il coinvolgimento di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p.

7.2.1. FATTISPECIE DELITTUOSE

Reati presupposto dell'illecito amministrativo di cui all'art. 24 D.Lgs. 231/01 emersi come potenzialmente rilevanti per la Società all'esito del Risk Assessment:

Malversazione a danno dello Stato (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto in modo lecito finanziamenti, sovvenzioni o contributi da parte dello Stato italiano o delle Comunità Europee per la realizzazione di opere o attività di interesse pubblico, non si proceda all'utilizzo delle somme per le finalità per cui sono state concesse.

Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)

La fattispecie criminosa si realizza nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri Enti pubblici o dalle Comunità Europee. A nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato si perfeziona nel momento dell'ottenimento dei finanziamenti.

Truffa a danno dello Stato (art. 640, comma 2, n. 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui si ottenga un ingiusto profitto ponendo in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato oppure ad altro Ente Pubblico. Il reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni supportate da documentazione artefatta, al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

Tale ipotesi di reato si configura se la truffa riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee. Tali fattispecie di reato potrebbero configurarsi allorquando un destinatario del Modello o altro soggetto tenuto al rispetto del Modello utilizzi ovvero presenti dichiarazioni o documenti falsi ovvero ometta informazioni dovute al fine di ottenere nell'interesse della Società, senza averne diritto, un contributo pubblico (ad es. per la partecipazione a corsi di formazione professionale o in relazione alle categorie di lavoratori c.d. "protette"). Tali fattispecie di reato potrebbero altresì configurarsi in ipotesi di concorso con un cliente allorquando un destinatario del Modello o altro soggetto tenuto al rispetto del Modello utilizzi ovvero presenti dichiarazioni o documenti falsi ovvero ometta informazioni dovute al fine di fare ottenere al cliente, senza averne diritto, un contributo pubblico.

Frode informatica (art. 640-ter)

La fattispecie di frode informatica consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati o programmi in essi contenuti, ottenendo un ingiusto profitto. Essa assume rilievo ai fini del D.Lgs. n. 231/2001 soltanto nel caso in cui sia

perpetrata ai danni dello Stato o di altro Ente Pubblico. In concreto, può integrarsi il reato in esame qualora, ad esempio, una volta ottenuto un finanziamento, venisse violato un sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente, oppure anche nel caso di modificazione delle risultanze di un conto corrente intestato ad un Ente pubblico, abusivamente accedendo ad un sistema di home banking.

Reati presupposto dell'illecito amministrativo di cui all'art. 25 D.Lgs. 231/01 emersi come potenzialmente rilevanti per la Società all'esito del Risk Assessment:

Corruzione per l'esercizio della funzione (art. 318 c.p.)

L'art. 318 c.p. incrimina la condotta del Pubblico Ufficiale ("PU") o, per effetto dell'art. 320 c.p., dell'Incaricato di un pubblico servizio ("IPS"), i quali ricevano indebitamente, per loro stessi o per un terzo, denaro o altra utilità o ne accettino la relativa promessa al fine di compiere atti che rientrano nell'esercizio delle loro funzioni o dei loro poteri.

L'oggetto dello scambio deve consistere in denaro o altra utilità (qualsiasi vantaggio materiale o morale, patrimoniale o non patrimoniale, che abbia valore per il pubblico agente).

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Tale reato si configura nel caso in cui un PU o, per effetto dell'art. 320 c.p., un IPS ricevano per loro stessi o per un terzo denaro o altra utilità o ne accettino la promessa, al fine di compiere (o per aver compiuto) un atto contrario ai doveri d'ufficio, ovvero per omettere o ritardare (o per avere omesso o ritardato) un atto del proprio ufficio. Per questa fattispecie valgono le considerazioni svolte per il reato di cui all'art. 318 c.p., con la precisazione che per "atto contrario ai doveri d'ufficio" si intende un concetto ampio nel quale rientrano sia gli atti che violano un obbligo specifico del pubblico funzionario, sia atti contrari al generico dovere di fedeltà, segretezza, onestà, vigilanza, imparzialità, obbedienza.

Corruzione in atti giudiziari (art. 319-ter c.p.)

L'elemento caratterizzante il reato di corruzione in atti giudiziari rispetto alle fattispecie appena esaminate è la finalità per cui gli atti corruttivi sono commessi: favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Il secondo comma dell'art. 319-ter c.p. prevede un aggravamento di pena in alcune ipotesi fondate sulle conseguenze sanzionatorie che derivano alla persona che subisce una condonna ingiusta quale effetto della condotta corruttiva.

Corruzione di persona incaricata a un pubblico servizio (art. 320 c.p.)

L'art. 320 c.p. prevede che le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

Per espresso richiamo della norma, in caso di condanna per il reato in esame troverà applicazione l'art. 32 quater, quindi l'applicazione della pena accessoria della incapacità di contrattare con la P.A.

Pene per il corruttore (art. 321 c.p.)

Le pene stabilite nel primo comma dell'art. 318, 319 e 319 bis, 319 ter e 320, in relazione alle suddette ipotesi di cui aglii articoli 318 e 319 si applicano anche a chi dà o promette al PU o all'IPC il denaro o altra utilità, ossia al c.d. corruttore.

Istigazione alla corruzione (art. 322 c.p.)

L'art. 322 c.p. prevede che le pene stabilite dagli artt. 318 e 319 c.p., ridotte di un terzo, si applichino anche a chi dà o promette indebitamente a un PU o ad un "PS denaro o altra utilità quando la dazione o la promessa non vengano accettate.

Traffico di influenze illecite (Art. 346-bis c.p.)

Il reato mira a perseguire tutte quelle condotte di intermediazione illecita poste in essere da chi, sfruttando relazioni esistenti con un pubblico ufficiale o un incarico di pubblico servizio, indebitamente fa dare o promettere, a sé o ad altri, denaro o altro vantaggio patrimoniale come prezzo della propria intermediazione illecita o come "tangente" necessaria per pagare il funzionario pubblico. In sostanza, nel primo caso il quantum rappresenta il corrispettivo dell'attività di intermediazione, nel secondo caso la "remunerazione" del pubblico funzionario.

Il reato si consuma al momento dell'accordo, non occorrendo l'effettiva dazione di denaro o altro vantaggio patrimoniale.

Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)

Il reato di cui all'art. 319-quater c.p. si configura, salvo che il fatto costituisca più grave reato, qualora un soggetto, al fine di trarre un indebito vantaggio, sia indotto da un PU o da un IPS, a dare o a promettere a questi o ad un terzo denaro o altra utilità. A differenza della costrizione prevista dall'art. 317 c.p. (che non determina la responsabilità penale del soggetto "costretto"), risponde del reato sia il PU/IPS sia la persona "indotta" laddove effettivamente, aderendo alla richiesta ricevuta, prometta o dia denaro o altra utilità al PU/IPS.

7.2.2. ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Le attività "sensibili" identificate dal Modello, nelle quali è maggiore il rischio che siano posti in essere comportamenti illeciti nei rapporti della Società con la Pubblica Amministrazione, sono le seguenti:

- gestione di comunicazioni e/o adempimenti nei confronti di Autorità di Vigilanza e\o di altri Enti Pubblici;
- gestione di comunicazioni e/o adempimenti per via telematica o utilizzando software pubblici;
- gestione di sistemi informativi aziendali o installazione, manutenzione, aggiornamento o gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici;
- ispezioni, verifiche o accertamenti da parte di Autorità di Vigilanza, Amministrazioni Pubbliche (INPS, INAIL, ENASARCO, etc.), Amministrazione Tributaria e/o Polizia Tributaria, Autorità competenti in materia di assunzione o cessazione del rapporto di lavoro, retribuzioni, ritenute e contributi previdenziali ed assistenziali dei dipendenti e dei collaboratori della Società;
- conclusione, stipulazione o esecuzione di contratti e/o convenzioni con Enti Pubblici, anche attraverso la partecipazione a procedure di evidenza pubblica;
- gestione di adempimenti fiscali;
- gestione dei rapporti con Enti Pubblici in occasione del rilascio di autorizzazioni, concessioni, licenze;
- gestione di adempimenti in materia di assunzione o cessazione del rapporto di lavoro, retribuzioni, ritenute e contributi previdenziali ed assistenziali dei dipendenti e dei collaboratori della Società;
- richiesta di contributi, sovvenzioni o finanziamenti pubblici in favore della Società e/o svolgimento di compiti di gestione amministrativo/contabile dei medesimi contributi e/o di rendicontazione nei confronti degli Enti concedenti;

- gestione dei contenziosi giudiziali e stragiudiziali (es. civili, tributari, giuslavoristici, amministrativi, penali, etc.), nomina dei legali e coordinamento delle loro attività.

In particolare, con riguardo alle fattispecie delittuose previste all'art. 24 del Decreto 231/01, le possibili modalità di realizzazione delle condotte sono:

- l'alterazione o la modifica di un software per la trasmissione in via telematica di dati alla P.A., con danno della stessa, o l'intervento (senza diritto) sui dati o sulle informazioni contenuti in un sistema della P.A., con danno della stessa;
- l'alterazione e/o la contraffazione della documentazione (ad esempio, il bilancio) da presentare ai fini della conclusione di contratti con la P.A. e/o ai fini della partecipazione ad una procedura ad evidenza pubblica e/o ai fini del rilascio di autorizzazioni, concessioni o licenze, procurando alla Società un ingiusto profitto con danno patrimoniale alla P.A.;
- l'impiego difforme dalla destinazione vincolata dei contributi, delle sovvenzioni o dei finanziamenti statali o comunitari;
- il conseguimento indebito di contributi, finanziamenti, mutui agevolati o altre erogazioni agevolate comunque denominate tramite l'utilizzo o la presentazione di dichiarazioni o documenti falsi o attestanti cose non vere ovvero tramite l'omissione di informazioni dovute;
- il conseguimento indebito di contributi, finanziamenti, mutui agevolati o altre erogazioni agevolate comunque denominate tramite l'alterazione e la contraffazione dei dati e della documentazione prescritta in sede di istruttoria per la concessione e della rendicontazione periodica dei finanziamenti agevolati.

Con riguardo, invece, alle fattispecie contenute nell'art. 25 del Decreto, le possibili modalità di realizzazione delle condotte criminose sono la dazione o promessa di denaro o di altra utilità (ad esempio, erogazione di servizi finanziari a condizioni diverse da quelle comunemente praticate alla clientela), anche per mezzo di altra funzione aziendale ovvero tramite consulenti/legali/fornitori esterni, al fine di indurre il funzionario pubblico al buon esito di adempimenti, verifiche e controlli cui è soggetta la Società, ove ne manchino i presupposti o attraverso procedure più rapide e semplificate rispetto alla prassi o contrarie ai doveri d'ufficio. Con particolare riferimento al reato di corruzione in atti giudiziari (art. 319-ter c.p.), le possibili modalità di realizzazione della condotta criminosa sono la dazione e/o la promessa di denaro o riconoscimento di altra utilità, anche per il tramite di legali esterni, al fine di influenzare l'andamento dei processi o dei procedimenti arbitrali a favore della Società o di danneggiare la controparte. Altra possibile modalità di realizzazione delle condotte

criminose di cui all'art. 25 del Decteto è, infine, individuabile nel processo di gestione e controllo delle note spese.

Con riguardo alle fattispecie delittuose sopra individuate, i soggetti\le Unità organizzative principalmente coinvolte sono:

- Amministratore Delegato;
- Direttore Finanza e Controllo;
- Funzioni aziendali di controllo;
- Unità Affari Legali e Societari;
- Unità Analisi di Gestione;
- Unità Finanza;
- Unità IT;
- Unità Rapporti con le AA.VV.

7.2.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Si riportano nel seguito, per le attività "sensibili" sopra individuate, i principi di controllo e di comportamento adottati dalla Società al fine di prevenire la commissione dei reati nei rapporti con la P.A., cui devono attenersi tutti i destinatari del Modello:

- trasparenza;
- segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con la P.A.;
- tracciabilità del processo, sia a livello di sistema informativo sia in termini documentali;
- divieto di diffondere informazioni non chiare, non corrette, false e fuorvianti;
- divieto di diffondere informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti;
- regolamentazione dei poteri di firma;
- divieto di adottare qualsiasi comportamento che induca a far credere di essere disposti ad elargire qualsivoglia utilità, fra cui omaggi in denaro, e comunque tale da indurre la controparte a ritenere plausibile la possibilità di ricevere, per sé o per altri, indebiti vantaggi, compiendo oppure omettendo o ritardando atti del suo ufficio;

- divieto di dare seguito, e conseguente obbligo immediato di segnalazione nei confronti del diretto superiore, a qualunque richiesta di indebiti vantaggi, o a qualunque tentativo di concussione, da parte di un soggetto della P.A. di cui dovesse essere destinatario, o semplicemente venire a conoscenza; il diretto superiore, a sua volta, ha l'obbligo di trasmettere la segnalazione ricevuta all'Unità Internal Audit per le valutazioni del caso e all'Organismo di Vigilanza;
- divieto di esprimere pareri personali sull'andamento della Società, ovvero sull'operatività della stessa e delle varie unità organizzative, senza la dovuta documentazione o sulla base di sensazioni non comprovabili;
- divieto di occultare, totalmente o parzialmente, informazioni;
- divieto di produrre o diffondere materiale artefatto;
- procedure autorizzative e di controllo delle spese;
- la presenza di denaro contante in misura sempre contenuta nelle casse della Società;
- divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del Decreto 231/01.

7.2.3.1. RICHIESTA DI INCONTRO DA PARTE DELLA PUBBLICA AMMINISTRAZIONE

L'iter procedurale previsto all'interno della Società volto alla regolamentazione del processo relativo alla gestione dei rapporti con la P.A., e in particolare alla gestione delle richieste di incontro provenienti dalla stessa, è basato sui seguenti presidi, in quanto applicabili (ovvero, tenuto conto delle procedure operative dell'Autorità richiedente):

- la gestione di tali incontri deve avvenire alla presenza di almeno due soggetti della Società;
- agli incontri con la P.A. è sempre prevista la partecipazione del Responsabile dell'Unità competente in materia e di almeno una funzione aziendale di controllo (Internal Audit, Compliance, Risk Management, Antiriciclaggio);
- predisposizione di un apposito report sintetico, sul contenuto degli incontri avvenuti, sottoscritto dal Responsabile dell'Unità competente in materia e dalla funzione aziendale di controllo che ne ha preso parte;
- la documentazione fornita durante gli incontri con la P.A. è sempre soggetta al vaglio dei soggetti che prendono parte agli incontri, nel rispetto del principio del doppio controllo;
- la documentazione fornita alla P.A. all'esito degli incontri è sempre soggetta al vaglio dei partecipanti all'incontro, nel rispetto del principio del doppio controllo;

- su copia della documentazione fornita alla P.A. all'esito degli incontri è sempre richiesto che vengano apposte la data e la sigla del soggetto competente (ovvero di colui che si è occupato della predisposizione della documentazione);
- copia della documentazione prodotta per la P.A., inclusa quella datata e siglata dal soggetto competente di cui al punto precedente, è sempre archiviata a cura del Responsabile dell'Unità competente in materia.

7.2.3.2. ISPEZIONE DELLA PUBBLICA AMMINISTRAZIONE

L'iter procedurale previsto all'interno della Società volto alla regolamentazione del processo relativo alla gestione delle ispezioni compiute dalla P.A., è basato sui seguenti presidi, in quanto applicabili tenuto conto delle procedure ispettive dell'Autorità:

- la gestione di tali ispezioni deve avvenire alla presenza di almeno due soggetti della Società;
- individuazione di un referente nei confronti della P.A., o di un responsabile della relazione con la stessa;
- partecipazione agli incontri di almeno una delle funzioni aziendali di controllo;
- predisposizione di un apposito report sintetico, sul contenuto degli incontri avvenuti, sottoscritto dalla funzione aziendale di controllo che ne ha preso parte, e dall'ulteriore partecipante, o dagli ulteriori partecipanti;
- tutta la documentazione consegnata alla P.A. nel corso degli incontri è sempre sottoposta al principio del doppio controllo;
- segnalazione all'Alta Direzione, da parte della funzione aziendale di controllo partecipante agli incontri, di eventuali comportamenti scorretti di funzionari della P.A. e/o di dipendenti della Società, ivi inclusi comportamenti concussivi e/o corruttivi;
- copia della documentazione fornita nel corso degli incontri alle P.A. è sempre archiviata a cura del referente nei confronti della P.A.\responsabile della relazione con la stessa.

Più in generale, con riguardo alle casistiche sopra individuate nell'ambito delle quali possono essere adottati atteggiamenti in contrasto con i principi di controllo e di comportamento previsti dalla Società, si segnalano:

- la presenza di denaro contante in misura sempre contenuta presso le casse della Società;
- l'obbligo, in capo a tutti i soggetti che chiedano un anticipo delle spese che sosterranno, di compilare apposita distinta per il rimborso, accompagnata da supporto documentale;

- il costante controllo dei flussi finanziari interni, strumento valido a far emergere gli atti di disposizione anomali delle disponibilità finanziarie della Società ad opera degli esponenti aziendali;
- l'adeguata conservazione, e la tenuta al riparo da possibili manipolazioni, delle registrazioni informatiche dei suddetti flussi finanziari, entrambe ausilio alla prevenzione dei generi di reato qui individuati.

La normativa interna e, in particolare, il Codice Etico e il Regolamento sulle operazioni personali, prevedono inoltre specifiche regole etiche ed appositi obblighi generali di comportamento per tutte le unità organizzative della Società. Tutti i soggetti interessati sono chiamati a firmare per presa visione ed accettazione i citati documenti, al pari di tutta la documentazione di autoregolamentazione; ogni successivo aggiornamento sarà invece comunicato a mezzo email.

7.3. REATI SOCIETARI

Le fattispecie delittuose contenute nella presente Parte Speciale sono costituite dai reati societari presenti nel Codice civile (agli artt. 2621 ss.); tali fattispecie risultano aggregate sulla base di criteri non del tutto omogenei sia per quanto attiene ai beni giuridici tutelati sia con riferimento alla scelta dei soggetti attivi (talvolta i soli amministratori, talaltre anche i direttori generali, i sindaci, i liquidatori e i dirigenti preposti alla redazione dei documenti contabili societari). Tuttavia, in ottica preventiva, la comune inerenza all'attività di impresa svolta in forma societaria ne giustifica una trattazione sistematica, tenendo conto che i reati societari, considerati nel loro complesso, mirano a tutelare i principi di trasparenza societaria, ovverosia la veridicità e la completezza dell'informazione societaria, di effettività del capitale sociale, di integrità del patrimonio, di correttezza della gestione del governo societario, nonché di tutela della concorrenza, del mercato e delle funzioni di controllo delle Autorità di vigilanza. Inoltre, l'obiettivo di tutela comune alle figure delittuose ivi contenute consiste nella protezione di una rosa di soggetti interni ed esterni alla società (tra cui i soci, i terzi e i creditori sociali, il mercato e la concorrenza), tutti interessati alle sorti e alla corretta gestione della medesima. Pertanto, il legislatore, attraverso l'inserimento dei reati societari nel novero dei reati-presupposto di cui al D.lgs. 231/2001, ha voluto sanzionare tutti quei comportamenti posti in essere a vantaggio o nell'interesse della società ma violando i principi anzidetti, così ledendo gli interessi dei soggetti che vantano un rapporto più o meno qualificato con la stessa o che hanno, nei confronti della medesima, obblighi di controllo.

Appartengono alle descritte categorie di reati le seguenti fattispecie (qui raggruppate, per semplicità, secondo categorie pressoché "omogenee"):

1. **condotte di falsificazione dell'informativa economica, finanziaria e patrimoniale afferente al bilancio, alle relazioni o ad altre comunicazioni sociali previste dalla legge** (art. 2621 c.c. "False comunicazioni sociali"; art. 2621 bis c.c. "Fatti di lieve entità");
2. **condotte distorsive della corretta gestione del governo societario** (art. 2625 comma 2 c.c. "Impedito controllo"; art. 2626 c.c. "Indebita restituzione dei conferimenti"; art. 2627 c.c. "Illegale ripartizione degli utili e delle riserve"; art. 2628 c.c. "Illecite operazioni sulle azioni o quote sociali o della società controllante"; art. 2629 c.c. "Operazioni in pregiudizio dei creditori"; art. 2629-bis c.c. "Omessa comunicazione del conflitto di interessi", art. 2632 c.c. "Formazione fittizia di capitale"; art. 2635 c.c. "Illecita influenza sull'assemblea");

3. **condotte distorsive della concorrenza** (art. 2635 c. 3 c.c. "Corruzione tra privati"; 2635-bis c.c. "Istigazione alla corruzione tra privati)**;**
4. **condotte distorsive del mercato e delle funzioni dell'Autorità di Vigilanza** (art. 2637 c.c. "Aggiotaggio", art. 2638 c.c. "Ostacolo all'attività delle funzioni pubbliche di vigilanza").

7.3.1. FATTISPECIE DELITTUOSE

Reati presupposto dell'illecito amministrativo di cui all'art. 25-ter D.Lgs. 231/01 emersi come potenzialmente rilevanti per la Società all'esito del Risk Assessment

False comunicazioni sociali (art. 2621 c.c.)

Il reato di cui all'art. 2621 c.c. incrimina gli amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori, che nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, al fine di conseguire per sé o per altri un ingiusto profitto, espongono consapevolmente fatti materiali rilevanti non rispondenti al vero, ovvero omettono fatti materiali rilevanti -la cui comunicazione è obbligatoria per legge- sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo ad indurre altri in errore.

Ai fini della sussistenza del reato di false comunicazioni sociali, dunque, le comunicazioni false o omesse devono riguardare la situazione economica, patrimoniale o finanziaria della società o del gruppo al quale appartiene e la condotta di falsificazione o di omissione deve essere concretamente idonea ad indurre altri in errore e volta al conseguimento di un profitto ingiusto.

Il reato si integra altresì qualora le comunicazioni false o omesse afferiscano a beni posseduti o amministrati dalla Società per conto di terzi.

La legge 69 del 2015, oltre ad aver ridisegnato il reato in esame - la cui disciplina è oggi contenuta in due articoli distinti, l'uno per le società non quotate (art. 2621 c.c.) e l'altro per le società quotate (art. 2622 c.c.) -, ha introdotto nell'art. 2621 bis c.c. due ipotesi in cui la pena è attenuata: la prima applicabile qualora i fatti risultino di lieve entità tenuto conto sia della natura e dimensioni della società che delle modalità o degli effetti della condotta; la seconda applicabile nel caso in cui i fatti siano commessi in relazione a società non sottoposte alle disposizioni sul fallimento e sul concordato preventivo (in tal caso è prevista una presunzione assoluta di lievità).

Inoltre, la riforma del 2015, circoscrivendo l'oggetto della falsità ai fatti materiali rilevanti non corrispondenti al vero, ha sollevato un contrasto giurisprudenziale sulla rilevanza penale del c.d. falso valutativo, precedentemente sanzionato al pari del falso materiale. La Cassazione, a Sezioni Unite,

intervenuta per dirimere la questione, ha concluso nel senso dell'attuale rilevanza penale del falso valutativo.

Fatti di lieve entità (art. 2621-bis, primo e secondo comma c.c.)

L'articolo in esame prevede l'applicazione della pena in forma attenuata da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Inoltre, al secondo comma, si afferma che si applica la medesima pena laddove i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.**Impedito controllo (art. 2625, secondo comma, c.c.)**

Tale figura delittuosa si integra qualora gli amministratori, occultando documenti o ponendo in essere altri idonei artifici, impediscano o comunque ostacolino lo svolgimento delle attività di controllo attribuite dalla legge ai soci o ad altri organi sociali, cagionando in tal modo un danno ai soci.
In assenza di danno, la condotta degli amministratori rileva esclusivamente quale illecito amministrativo, non rientrante nel novero dei reati presupposto ai sensi del d.lgs. 231/2001.
Inoltre, al terzo comma, è previsto un aggravamento di pena qualora il fatto riguardi una società quotata.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

Il reato di cui all'art. 2626 c.c. incrimina la condotta degli amministratori che restiuiscano, fuori dai casi di legittima riduzione del capitale, anche simulatamente, i conferimenti ai soci, ovvero che li liberino dall'obbligo di eseguirli, sempre che il fatto cagioni un danno consistente nella riduzione del patrimonio netto ad un valore inferiore al capitale nominale.

La restituzione può essere eseguita in qualsiasi forma, può essere integrale o parziale, palese o simulata.

Si precisa che la condotta difficilmente potrà essere realizzata nell'interesse o a vantaggio dell'ente, avendo quale effetto un pregiudizio per la società consistente in una lesione patrimoniale.

Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)

Tale fattispecie delittuosa sanziona, a titolo contravvenzionale, la condotta degli amministratori nel

caso in cui essi ripartiscano utili o acconti su utili non conseguiti o destinati per legge a riserva o distribuiscano riserve che non possono per legge essere ripartite. **Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)**

Il reato di cui all'art. 2628 c.c. si configura qualora gli amministratori, fuori dai casi consentiti dalla legge, acquistino o sottoscrivano azioni o quote sociali ovvero della società controllante determinando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

All'ultimo comma è prevista una causa estintiva del reato consistente nella ricostituzione del capitale o delle riserve indisponibili prima del termine stabilito per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Il reato di cui all'art. 2629 c.c. sanziona gli amministratori che, violando le disposizioni di legge a tutela dei creditori, effettuano riduzioni di capitale sociale, fusioni con altra società o scissioni, cagionando un danno ai creditori.

Ai fini dell'integrazione del reato è necessario che l'evento del reato consistente nel pregiudizio ai creditori sia conseguenza causale di una delle operazioni sopra indicate. Il reato si estingue qualora i creditori siano risarciti prima dell'instaurazione del giudizio.

Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)

La fattispecie in esame disciplina l'ipotesi in cui l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1 settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, o del decreto legislativo 21 aprile 1993, n. 124, violi gli obblighi previsti dall'articolo 2391, primo comma.

Si prevede che egli è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.

Formazione fittizia del capitale (art. 2632 c.c.)

La norma punisce la condotta degli amministratori e dei soci conferenti i quali, anche in parte, formano

od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

Corruzione tra privati (art. 2635, comma 3, c.c.)

Il reato di cui all'art. 2635 c.c., al terzo comma, incrimina la condotta di colui che offre, promette o dà denaro o altra utilità agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, a chi, nell'ambito organizzativo della società o dell'ente privato, esercita funzioni direttive diverse da quelle proprie dei soggetti appena menzionati nonché a coloro che sono sottoposti alla direzione o alla vigilanza di detti soggetti, affinché, per sé o per altri, compiano o omettano atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.
La condotta tipica di offerta, promessa o dazione può essere realizzata sia direttamente dai soggetti apicali della società o da subordinati, sia indirettamente per interposta persona.
Considerato che il d.lgs. 231 del 2001 richiama esclusivamente il terzo comma dell'art. 2635 c.c. nell'elenco dei reati presupposto, l'eventuale responsabilità dell'ente verrà in gioco solo qualora i predetti soggetti agiscano come corruttori, non anche quando siano stati corrotti.

Istigazione alla corruzione tra privati (art. 2635-bis, comma 1, c.c.)

Il reato di cui all'art. 2635-bis, al primo comma, c.c. incrimina la condotta di colui che offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società ed enti privati nonché a chi svolge nell'ambito degli stessi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà qualora l'offerta o la promessa non venga accettata

Illecita influenza sull'assemblea (art. 2636 c.c.)

La fattispecie di reato in menzione si realizza qualora con atti simulati o fraudolenti, si determini la maggioranza in assemblea, allo scopo di procurare a sè o ad altri un ingiusto profitto.
Per la condotta in questione si prevede la pena della reclusione da sei mesi a tre anni.

Aggiotaggio (art. 2637 c.c.)

L'art. 2637 c.c. sanziona con la pena della reclusione da uno a cinque anni chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza (art. 2638 c.c.)

Il reato di cui all'art. 2638 c.c. si configura nell'ipotesi in cui, al fine di ostacolare l'attività delle autorità pubbliche di vigilanza e di garanzia (incluse, queste ultime, nel perimetro applicativo dalla giurisprudenza), gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza e di garanzia, o tenuti ad obblighi nei loro confronti, rappresentino alle predette autorità -nelle comunicazioni previste dalla legge- fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, in merito alla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero occultino fraudolentemente in tutto o in parte fatti che avrebbero dovuto esporre, concernenti la situazione medesima, anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Il reato si integra, altresì, in via residuale, qualora venga posta in essere qualsiasi condotta attiva od omissiva che determini concretamente un ostacolo all'esercizio delle funzioni proprie dell'autorità di vigilanza e di garanzia.
La pena è raddoppiata se il reato è commesso in relazione a società quotate ovvero ad emittenti con strumenti finanziari diffusi tra il pubblico in maniera rilevante.

Falso in prospetto (art. 173-bis D.Lgs. n. 58/1998)

La Legge 262/2005 (cosiddetta "Legge sul Risparmio") ha abrogato l'art. 2623 c.c., concernente il falso in prospetto, sostituendolo con una nuova fattispecie inserita all'interno del corpo normativo del Testo Unico delle disposizioni in materia di intermediazione finanziaria di cui al D.Lgs. n. 58/1998 (di seguito T.U.F.). Il nuovo art. 173 bis del T.U.F. punisce la condotta di chi espone false informazioni od occulta dati o notizie nei prospetti richiesti ai fini della sollecitazione al pubblico risparmio o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in

occasione delle offerte pubbliche di acquisto o di scambio. Affinché tale condotta integri gli estremi del reato, è indispensabile che il soggetto che la pone in essere agisca con l'intenzione di ingannare i destinatari dei prospetti, al fine di conseguire un ingiusto profitto, per sé o per altri. Occorre altresì che le informazioni false od omesse siano idonee ad indurre in errore i loro destinatari. Poichè la Legge sul Risparmio non è intervenuta sul testo dell'art. 25 ter del D.Lgs. n. 231/2001, sostituendo espressamente il richiamo all'art. 2623 c.c. in esso contenuto con quello all'art. 173-bis del T.U.F., si pongono seri dubbi sulla configurabilità della responsabilità amministrativa degli Enti a fronte della commissione del reato punito da tale nuova fattispecie, rispetto alla quale, peraltro, anche prescidendo dall'effettiva sua attribuibilità all'Ente, la Società si è comunque dotata di specifici protocolli preventivi nell'ambito del più ampio corpus normativo adottato al proprio interno, cui si è fatto cenno nella Parte Generale.

7.3.2. ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Le attività "sensibili" identificate dal Modello, nelle quali è maggiore il rischio che siano posti in essere i reati societari sopra illustrati, sono le seguenti:

- gestione di comunicazioni e/o adempimenti nei confronti di Autorità di Vigilanza e/o di altri Enti Pubblici;
- ispezioni, verifiche o accertamenti da parte di Autorità di Vigilanza, Amministrazioni Pubbliche (INPS, INAIL, ENASARCO, etc.), Amministrazione Tributaria e/o Polizia Tributaria, Autorità competenti in materia di assunzione o cessazione del rapporto di lavoro, di retribuzioni, di ritenute e contributi previdenziali ed assistenziali dei dipendenti e dei collaboratori della Società;
- gestione di adempimenti fiscali;
- gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione relativamente alle verifiche sulla gestione amministrativa e contabile e sul bilancio di esercizio;
- gestione delle comunicazioni sociali, sia con riferimento alla Società che agli OICR gestiti (bilanci, relazioni, o altre comunicazioni sociali previste dalla legge, dirette ai soci, ai creditori o al pubblico);
- predisposizione di prospetti, note o documentazione da sottoporre, o mettere a disposizione, degli amministratori, in occasione delle sedute del Consiglio di Amministrazione, o dei soci in occasione delle Assemblee, e – più in generale, gestione delle stesse;
- collaborazione nella predisposizione delle situazioni patrimoniali o dei prospetti in occasione della deliberazione o dell'esecuzione di operazioni straordinarie o di operazioni sul capitale;

- supporto al Consiglio di Amministrazione nelle deliberazioni riguardanti la destinazione dell'utile d'esercizio;
- imputazione o esecuzione per conto della Società di ordini di acquisto o vendita di strumenti finanziari (tesoreria);
- le funzioni di controllo partecipano al processo di monitoraggio, istruttoria e segnalazione delle eventuali operazioni sospette di abuso di mercato;
- predisposizione dei prospetti richiesti ai fini della sollecitazione al pubblico risparmio;
- deliberazioni del Consiglio di Amministrazione, dell'Assemblea dei Soci e dei vari Comitati esistenti all'interno della Società;
- attività ordinaria dei soggetti appartenenti alla Direzione Commerciale e alle Unità Consulenza, Trading Desk e Ricezione e Trasmissione Ordini (RTO) e Operations (Amministrazione Clienti);
- rapporti negoziali con gli enti privati, soprattutto nello svolgimento delle seguenti attività:
  - raccolta di fondi per l'investimento nei prodotti e servizi della Società e, in generale, tutti i rapporti con gli investitori;
  - gestione dei rapporti con enti privati certificatori, nazionali o internazionali;
  - acquisto di beni e servizi e, in generale, la negoziazione, la stipula e l'esecuzione di contratti con soggetti privati;
  - gestione dei rapporti con operatori bancari e creditizi;
  - gestione dei contratti di consulenza e prestazione professionale.

Con specifico riguardo al reato di cui all'art. 2638, commi 1 e 2, c.c. (Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza), le possibili modalità di realizzazione delle condotte criminose sono le seguenti:

- esposizione, nelle comunicazioni alle Autorità di Vigilanza e/o ad altri Enti Pubblici previste in base alla legge, di fatti non rispondenti al vero concernenti la situazione economica, patrimoniale e finanziaria della Società;
- occultamento con mezzi fraudolenti, nelle comunicazioni alle Autorità di Vigilanza e/o ad altri Enti Pubblici previste in base alla legge, di fatti concernenti la situazione economica, patrimoniale e finanziaria della Società;
- adozione di condotte ostruzionistiche o non collaborative nei confronti delle Autorità di Vigilanza, Amministrazioni Pubbliche (INPS, INAIL, ENASARCO, etc.), Amministrazione Tributaria e/o Polizia Tributaria, Autorità competenti in materia di assunzione o cessazione

del rapporto di lavoro, di retribuzioni, di ritenute e contributi previdenziali ed assistenziali dei dipendenti e dei collaboratori della Società, al fine di ostacolarne le funzioni.

Con riguardo al reato di cui all'art. 2621 c.c. (False comunicazioni sociali in danno dei soci o dei creditori), le possibili modalità di realizzazione delle condotte criminose sono le seguenti:

- alterazione, da parte degli Amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori della Società (o da parte di altri soggetti in concorso con i titolari delle predette funzioni) della situazione economica, patrimoniale o finanziaria della Società o del Gruppo cui essa appartiene in modo concretamente idoneo ad indurre in errore i soggetti terzi tramite esposizione in bilancio di poste di bilancio (non valutative) inesistenti o di valore difforme da quello reale, ovvero occultamento di fatti rilevanti tali da mutare la rappresentazione delle effettive condizioni economiche della Società;
- alterazione di prospetti, note o documentazione da sottoporre, o mettere a disposizione, degli amministratori, in occasione delle sedute del Consiglio di Amministrazione, o dei soci in occasione delle Assemblee, e – più in generale, gestione delle stesse.

Condotte criminose possono essere realizzate anche nell'ambito della gestione dei rapporti infragruppo, sia quelli in essere all'interno del gruppo Kairos, sia quelli esistenti con la controllante JB; durante le operazioni di calcolo del valore delle quote degli OICR gestiti; nell'ambito della gestione delle risorse finanziarie, in primis da parte del Direttore Finanza e Controllo e dell'Unità Finanza; nell'ambito della gestione degli adempimenti fiscali, in primis ad opera del Direttore Finanza e Controllo e dell'Unità Finanza, nonché, infine, in caso di omaggi, regali, spese di rappresentanza e sponsorizzazioni ad opera di tutte le unità di business, oltre che dell'Unità Compliance.Con riguardo al reato di cui all'art. 2627 c.c. (Illegale ripartizione degli utili e delle riserve), le possibili modalità di realizzazione delle condotte criminose sono, in concorso con gli Amministratori della Società, la ripartizione di utili o non effettivamente conseguiti o destinati per legge a riserva ovvero la ripartizione di riserve, anche non costituite con utili, non distribuibili per legge.

Per quanto concerne lo specifico reato di aggiotaggio (art. 2637 c.c.), le possibili modalità di realizzazione della condotta criminosa sono la diffusione di notizie false o il compimento di operazioni simulate (operazioni che le parti non abbiano inteso in alcun modo realizzare e/o operazioni che presentino un'apparenza difforme rispetto a quelle effettivamente volute) o altri artifici in modo da

provocare sensibili alterazioni del prezzo di strumenti finanziari non quotati o per i quali non sia stata richiesta l'ammissione a quotazione in Italia o in mercati regolamentati dell'UE.

Per quanto concerne i reati previsti dall'art. 2625, comma 2, c.c. (Impedito controllo), le possibili modalità di realizzazione della condotta criminosa sono l'occultamento di documenti, l'adozione di atteggiamenti ingiustificatamente dilatori ovvero la realizzazione di artifici idonei ad impedire od ostacolare il controllo da parte del Collegio Sindacale, della Società di Revisione e dei soci (nei casi previsti dalla legge), nell'interesse o a vantaggio della Società.

Con riguardo al reato di cui all'art. 2636 c.c. (Illecita influenza sull'Assemblea), le possibili modalità di realizzazione della condotta criminosa sono:

- la simulazione o fraudolenta predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'Assemblea, anche in concorso con altri, al fine di consentire l'assunzione di delibere a vantaggio e nell'interesse della Società, ma in spregio dei diritti delle minoranze o in modo tale da alterare la corretta dialettica tra gli organi sociali;
- l'esecuzione di atti (simulati o fraudolenti) tali da far convergere la maggioranza assembleare verso tesi precostituite, al fine di consentire l'assunzione di delibere a vantaggio e nell'interesse della Società, ma in spregio dei diritti delle minoranze o in modo tale da alterare la corretta dialettica tra gli organi sociali.

Con riferimento al reato di falsità nelle relazioni o nelle comunicazioni delle Società di Revisione (art. 2624, comma 1, c.c.), le possibili modalità di realizzazione della condotta criminosa sono, in concorso con i revisori, la falsa attestazione o l'occultamento – nelle relazioni o in altre comunicazioni – di informazioni concernenti la situazione economica, patrimoniale o finanziaria della Società, con l'intento di ingannare i destinatari delle comunicazioni ed in modo idoneo ad indurli in errore circa la predetta situazione, al fine di conseguire per sé o per altri un ingiusto profitto.

Per quanto riguarda il reato di cui all'art. 2628 c.c. (Illecite operazioni sulle azioni o quote sociali o della società controllante), le possibili modalità di realizzazione della condotta criminosa sono, in concorso con gli Amministratori della Società, l'acquisto o sottoscrizione di azioni o quote sociali o della Società controllante al di fuori dei casi consentiti dalla legge, in modo tale da causare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Con riferimento al reato di cui all'art. 2629 c.c. (Operazioni in pregiudizio dei creditori), le possibili modalità di realizzazione della condotta criminosa sono, in concorso con gli Amministratori della

Società, l'esposizione di dati idonei a pregiudicare i diritti dei creditori sociali in occasione di operazioni di riduzione del capitale sociale, di fusione o di scissione, nell'interesse e a vantaggio della Società.

Con riferimento al reato di cui all'art. 2629-bis c.c. (Omessa comunicazione del conflitto di interessi), le possibili modalità di realizzazione della condotta criminosa consistono nell'alterazione di prospetti, note o documentazione da sottoporre, o mettere a disposizione, degli amministratori, in occasione delle sedute del Consiglio di Amministrazione, o dei soci in occasione delle Assemblee, e – più in generale, gestione delle stesse. Condotte criminose possono essere realizzate anche nell'ambito della gestione delle risorse finanziarie, in primis da parte del Direttore Finanza e Controllo e dell'Unità Finanza, nonché nell'ambito della gestione di omaggi, regali, spese di rappresentanza e sponsorizzazioni da parte di tutte le unità di business, oltre che dell'Unità Compliance.

Le possibili modalità di realizzazione della condotta criminosa relativa al reato di indebita restituzione dei conferimenti (art. 2626 c.c.) sono, in concorso con gli Amministratori della Società, la restituzione ad uno o più soci, anche per via indiretta o simulata, dei conferimenti e/o liberazione dei soci medesimi dall'obbligo di eseguirli, nell'interesse e a vantaggio della Società.

Con riguardo, infine, al reato di formazione fittizia del capitale (art. 2632 c.c.), le possibili modalità di realizzazione della condotta criminosa sono, in concorso con gli Amministratori della Società e al fine di fornire all'esterno un'apparente situazione di solidità patrimoniale della medesima, la costituzione o l'aumento del capitale sociale in modo fittizio, attraverso l'attribuzione di azioni per somma inferiore al loro valore nominale o la sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti.

Con riguardo alla fattispecie di corruzione tra privati (art. 2635 c.c.), il rischio di commissione del reato si annida in tutte le relazioni negoziali con partner commerciali, finanziari o industriali, rispetto alle quali l'interesse di controparte è normalmente rivolto alla massimizzazione dei profitti, attraverso un incremento dei rapporti contrattuali e/o l'ottenimento delle condizioni negoziali economicamente più vantaggiose. Il rischio potenziale di commissione del reato, in particolare, si colloca nell'eventualità che tali (legittimi) obiettivi d'impresa siano perseguiti attraverso comportamenti corruttivi – cioè attraverso la dazione o la promessa di denaro o altre utilità nei confronti di esponenti aziendali (apicali o subordinati) di controparte – funzionali ad ottenere, grazie al comportamento infedele del privato corrotto, la massimizzazione di vantaggi e profitti nell'interesse della Società. Condotte criminose possono essere realizzate anche nell'ambito della gestione delle risorse finanziarie, in primis da parte del Direttore Finanza e Controllo e dell'Unità Finanza (e ciò con riguardo anche alla fattispecie della istigazione alla corruzione fra privati (art. 2635-bis c.c.), nonché in quello della gestione di omaggi,

regali, spese di rappresentanza e sponsorizzazioni (e ciò con riguardo anche alla fattispecie della istigazione alla corruzione fra privati (art. 2635-bis c.c.).

Nell'ambito delle attività della Società, tale situazione di rischio potrebbe presentarsi, ad esempio, nei rapporti con gli intermediari (quali, a titolo esemplificativo, i negoziatori), oppure con le società prodotto con le quali la Società potrebbe stipulare accordi per la loro distribuzione, i cui esponenti aziendali, nel corso di incontri con gli operatori della Società, potrebbero essere allettati dalla promessa, diretta o indiretta, di qualsivoglia utilità personale, allo scopo di agevolare o incrementare i rapporti in essere presso la Società.

Con riguardo alle fattispecie delittuose sopra individuate, i soggetti\le Unità organizzative principalmente coinvolte sono:

- Consiglio di Amministrazione;
- Amministratore Delegato;
- Direttore Finanza e Controllo;
- Funzioni aziendali di controllo;
- Unità Affari Legali e Societari;
- Direzione Commerciale;
- Unità Operations (Amministrazione Clienti);
- Unità Consulenza;
- Unità Trading Desk e RTO;
- Unità Finanza;
- Unità Analisi di Gestione;
- Unità Rapporti con le AA.VV.

7.3.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

7.3.3.1. GESTIONE DEI RAPPORTI CON LE AUTORITÀ DI VIGILANZA

Il processo relativo alla gestione dei rapporti con le AA.VV. in occasione di:

- elaborazione e trasmissione delle segnalazioni occasionali o periodiche;
- riscontri ed adempimenti connessi a richieste/istanze di dati e notizie provenienti dalle AA.VV.,

è presidiato da un sistema di controlli basato sui seguenti principi:

- trasparenza;
- registrazione della corrispondenza in entrata e in uscita da e verso le AA.VV.;
- istituzione di una unità appositamente deputata ai rapporti con le AA.VV.;
- divieto di diffondere informazioni non chiare, non corrette, false e fuorvianti;
- divieto di diffondere informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti;
- divieto di occultare, totalmente o parzialmente, informazioni;
- divieto di produrre e diffondere materiale artefatto;
- implementazione di sistemi di sicurezza logica e di altre procedure a garanzia della corretta gestione delle informazioni;
- obbligo di fornire tutte le informazioni richieste senza alcuna omissione, chiedendo eventuali delucidazioni agli uffici competenti dell'Autorità di Vigilanza richiedente qualora emergessero dubbi interpretativi o procedurali;
- obbligo di trasmettere puntualmente le segnalazioni periodiche alle Autorità di Vigilanza e tempestivamente riscontrare le richieste/istanze pervenute dalle stesse Autorità;
- obbligo di documentare/registrare in via informatica, ed archiviare presso la struttura di competenza, ogni comunicazione nei confronti delle Autorità di Vigilanza avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della SGR;
- monitoraggio da parte delle funzioni di controllo della corrispondenza in entrata e in uscita da e verso le AA.VV.;
- monitoraggio da parte della Società di Revisione della corrispondenza in entrata e in uscita da e verso le AA.VV.;
- regolamentazione dei poteri di firma.

7.3.3.1.1. ELABORAZIONE E TRASMISSIONE DELLE SEGNALAZIONI

L'iter procedurale previsto all'interno della SGR per la regolamentazione del processo relativo all'elaborazione e trasmissione delle segnalazioni è basato sui seguenti presidi:

- definizione di un'apposita unità all'interno della SGR responsabile delle segnalazioni nei confronti delle Autorità di Vigilanza. Nello specifico:
    - l'unità responsabile delle segnalazioni statistiche è l'Unità Finanza;
    - il responsabile delle cosiddette segnalazioni "SARA" è la Funzione Antiriciclaggio;

- l'unità responsabile delle segnalazioni diverse da quelle statistiche, riferibili ai prodotti e alla contabilità societaria, e dalle "SARA", è l'Unità Rapporti con le AA.VV., unica titolare dell'accesso previsto alla "Teleraccolta";

- nel rispetto del principio del doppio controllo, le segnalazioni statistiche riferibili ai prodotti sono elaborate in parte dalla banca depositaria BNP Paribas e in parte dall'outsourcer – Xchanging Italy S.p.A. – con il contributo dell'Unità Operations per i dati che non risiedono sul sistema dell'outsourcer. I dati vengono, poi, aggregati da parte della banca depositaria BNP Paribas e da questa trasmessi all'outsourcer – Xchanging Italy S.p.A. – che provvede ad elaborare la segnalazione secondo i criteri dettati dalla normativa Banca d'Italia e ad inviarla alla stessa attraverso l'applicativo Infostat. Il controllo di primo livello viene eseguito dall'outsourcer Xchanging Italy S.p.A., anche sulla base delle risultanze del diagnostico di sistema, mentre il controllo di secondo livello viene eseguito dall'Unità Finanza;
- nel rispetto del principio del doppio controllo, le segnalazioni "SARA" sono elaborate dall'outsourcer – Xchanging Italy S.p.A. – e controllate da quest'ultimo, quale controllo di primo livello, nonché verificate dalla Funzione Antiriciclaggio, quale controllo di secondo livello;
- nel rispetto del principio del doppio controllo, le segnalazioni statistiche riferibili ai dati della contabilità societaria sono predisposte tramite il sistema dell'outsourcer in maniera semi-automatica sulla base delle informazioni e dei dati forniti dall'Unità Finanza e verificate dall'outsourcer, quale controllo di primo livello, nonché dall'Unità Finanza, quale controllo di secondo livello;
- le segnalazioni statistiche riferite ai "Fondi propri" sono predisposte dall'outsourcer – Xchanging Italy S.p.A. – sulla base delle informazioni e dei dati forniti dall'Unità Finanza e, nel rispetto del principio del doppio controllo, verificate dall'Unità Risk Management per quanto concerne l'attendibilità delle risultanze numeriche;
- le segnalazioni diverse da quelle statistiche e dalle "SARA" sono controllate, nel rispetto del principio del doppio controllo,
  - dal Responsabile dell'Unità Rapporti con le AA.VV., quando effettuate dall'addetto dell'unità medesima;
  - dall'addetto dell'Unità Rapporti con le AA.VV., quando effettuate da un soggetto non appartenente a quest'ultima unità;
- la documentazione riferita alle varie segnalazioni è conservata, mediante archiviazione cartacea e/o elettronica, dal soggetto che ha effettuato il controllo.

7.3.3.1.2. RISCONTRI A RICHIESTE DI DATI E NOTIZIE

L'iter procedurale previsto all'interno della SGR per la regolamentazione del processo relativo ai riscontri connessi a richieste/istanze di dati e notizie è basato sui seguenti presidi:

- definizione di un'apposita unità dedicata ai rapporti con le AA.VV.: l'Unità Rapporti con le Autorità di Vigilanza;
- vigilanza, da parte delle funzioni di controllo, sul corretto adempimento di quanto richiesto, a mezzo di richieste e istanze, da parte delle AA.VV.;
- apposizione della sigla, da parte dei soggetti coinvolti nella redazione delle risposte da inoltrare alle AA.VV., sulla risposta o sulla documentazione prodotta di propria spettanza;
- la lettera di risposta, nonché la relativa documentazione allegata, sono controllate dal Responsabile dell'Unità Compliance, che appone la propria sigla sulla lettera stessa;
- copia della lettera di risposta e della documentazione inoltrate alle AA.VV. sono archiviate da parte dell'Unità Rapporti con le Autorità di Vigilanza, che conserva anche quanto siglato da tutti i soggetti coinvolti nel processo.

7.3.3.2. GESTIONE DEI RAPPORTI CON IL COLLEGIO SINDACALE E CON LA SOCIETÀ DI REVISIONE

Il processo relativo alla gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione è presidiato da un sistema di controlli basato sui seguenti principi:

- trasparenza;
- diffusione delle informazioni;
- individuazione dei soggetti tenuti a intrattenere rapporti con il Collegio Sindacale e la Società di Revisione;
- divieto di adottare qualsiasi comportamento che induca a far credere di essere disposti ad elargire qualsivoglia utilità, fra cui omaggi in denaro, e comunque tale da indurre la controparte a ritenere plausibile la possibilità di ricevere, per sé o per altri, indebiti vantaggi, compiendo oppure omettendo o ritardando atti del suo ufficio;
- divieto di diffondere informazioni non chiare, non corrette, false e fuorvianti;
- divieto di diffondere informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti;
- divieto di produrre e diffondere materiale artefatto;

- divieto di esprimere pareri personali sull'andamento della Società, ovvero sull'operatività della stessa e delle varie unità organizzative, senza la dovuta documentazione o sulla base di sensazioni non comprovabili;
- procedure organizzative di controllo di primo e secondo livello (principio del "doppio controllo").

L'iter procedurale previsto all'interno della SGR per la regolamentazione del processo relativo alla gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione, e in particolare finalizzato ad evitare il compimento del reato dell'impedito controllo, è basato sui seguenti presidi:

- individuazione di un'interfaccia, o di un responsabile della relazione con il Collegio Sindacale e la Società di Revisione. Il referente individuato, sia per il Collegio Sindacale che per la Società di Revisione, è:
    - con riferimento ai servizi/attività di investimento, i Responsabili dell'Unità Compliance, dell'Unità Internal Audit e dell'Unità Risk Management, ciascuno per quanto di propria competenza;
    - con riferimento alla contabilità societaria, il Responsabile dell'Unità Finanza;
    - con riferimento ai dati di carattere gestionale, alle commissioni attive e passive, alle componenti variabili delle remuneraziioni, il Responsabile dell'Unità Analisi di Gestione;
    - con riferimento alla contabilità prodotti, il Responsabile dell'Unità Operations;
- agli incontri con il Collegio Sindacale e la Società di Revisione è sempre prevista la partecipazione di almeno due soggetti.

Per quanto concerne i rapporti con il Collegio Sindacale:

- tutta la documentazione consegnata al Collegio Sindacale è sempre sottoposta al principio del doppio controllo, vagliata dal competente responsabile della relazione con il Collegio Sindacale (Responsabili dell'Unità Compliance, dell'Unità Internal Audit, dell'Unità Risk Management, Responsabile dell'Unità Finanza, Responsabile dell'Unità Analisi di Gestione, o Responsabile dell'Unità Operations);
- tutta la documentazione consegnata brevi manu al Collegio Sindacale, sia in occasione degli incontri, sia precedentemente o successivamente agli incontri, è datata e siglata dalla funzione

che ne ha curato la predisposizione. Di tale documentazione deve essere inoltrata copia al Responsabile del'Unità Internal Audit che ne provvede all'archiviazione in forma elettronica;

- quando la documentazione è inoltrata a mezzo e-mail, è rintracciabile elettronicamente la data e la funzione che ne ha curato la predisposizione. In tal caso, il Responsabile dell'Unità Internal Audit deve essere messo in copia nella e-mail, in modo da avere evidenza della documentazione trasmessa elettronicamente;
- segnalazione all'Alta Direzione, in primis da parte del responsabile della relazione con il Collegio Sindacale e – in seconda battuta – in maniera indipendente – dagli altri soggetti coinvolti, qualora ne vengano a conoscenza, di eventuali comportamenti scorretti di dipendenti della Società nell'ambito degli incontri o nell'invio della documentazone richiesta.

Per quanto riguarda i rapporti con la Società di Revisione, tenuto conto dell'elevato numero di documenti che vengono forniti alla stessa, la procedura che segue si applica alla documentazione che ha natura rilevante per le finalità a cui la stessa è mirata:

- la documentazione consegnata alla Società di Revisione è sempre sottoposta al principio del doppio controllo e vagliata dal competente responsabile della relazione con la Società di Revisione (Responsabile dell'Unità Compliance, o dell'Unità Internal Audit, o dell'Unità Risk Management, Responsabile dell'Unità Finanza, Direttore Finanza e Controllo o Responsabile dell'Unità Operations);
- la documentazione consegnata brevi manu alla Società di Revisione, sia in occasione degli incontri, sia precedentemente o successivamente agli incontri, è datata e siglata dalla funzione che ne ha curato la predisposizione. Di tale documentazione deve essere inoltrata copia al Responsabile del'Unità Internal Audit, che ne provvede all'archiviazione elettronica;
- laddove la documentazione sia inoltrata a mezzo e-mail, è rintracciabile elettronicamente la data e la funzione che ne ha curato la predisposizione. In tal caso, il Responsabile del'Unità Internal Audit deve essere messo in copia nella e-mail in modo da avere evidenza della documentazione trasmessa elettronicamente;
- segnalazione all'Alta Direzione, in primis da parte del responsabile della relazione con la Società di Revisione, e, in seconda battuta, in maniera indipendente, dagli altri soggetti coinvolti, qualora ne vengano a conoscenza, di eventuali comportamenti scorretti di dipendenti della Società nell'ambito degli incontri o nell'invio della documentazone richiesta.

L'iter procedurale previsto all'interno della SGR per la regolamentazione del processo relativo alla gestione dei rapporti con la Società di Revisione con riferimento alla certificazione del Bilancio societario ed alle verifiche periodiche, in particolare finalizzato ad evitare il compimento del reato delle false comunicazioni sociali, è basato sui seguenti presidi, che, tenuto conto dell'elevato numero di documenti che vengono forniti alla Società di Revisione, si intendono applicati alla documentazione che abbia natura rilevante per le finalità a cui la procedura stessa è mirata:

- individuazione del Responsabile dell'Unità Finanza e del Direttore Finanza e Controllo quali unici interlocutori nei confronti della Società di Revisione in tema di comunicazioni sociali, come poc'anzi illustrato;
- la documentazione consegnata alla Società di Revisione è sottoposta al principio del doppio controllo. La documentazione richiesta dalla Società di Revisione, ed a questa trasmessa a mezzo e-mail, è archiviata in formato elettronico rispettivamente dall'Unità Finanza o dalla Direzione Finanza e Controllo. La documentazione consegnata, invece, brevi manu alla Società di Revisione viene vagliata a seconda della competenza dal Responsabile dell'Unità Finanza o dal Direttore Finanza e Controllo;
- la documentazione predisposta dalla Società di Revisione con riferimento al Bilancio societario è inoltrata al Responsabile dell'Unità Finanza o al Direttore Finanza e Controllo, che, se richiesto, esprimono il proprio giudizio a mezzo email;
- verificata, da parte del Responsabile dell'Unità Finanza, la congruità fra la Relazione di certificazione e il Bilancio, la documentazione é inoltrata all'Alta Direzione;
- i documenti costituenti il pacchetto di Bilancio e la Relazione di certificazione al Bilancio stesso sono archiviati a cura dell'Unità Finanza;
- segnalazione all'Alta Direzione, ad opera del Responsabile dell'Unità Finanza, di eventuali comportamenti scorretti di dipendenti della SGR nei confronti della Società di Revisione di cui sia venuto a conoscenza.

Il Codice Etico e il Regolamento sulle operazioni personali, ai quali si rimanda, prevedono specifiche regole etiche e appositi obblighi generali di comportamento per tutte le unità organizzative della SGR. Con riguardo ai rapporti della Società con soggetti esterni, il Codice Etico stabilisce che essi debbano svolgersi con la massima correttezza, integrità e indipendenza, evitando anche di dare l'impressione di voler influenzare impropriamente le decisioni della controparte o di richiedere trattamenti di favore.

7.3.3.3. GESTIONE DELLE COMUNICAZIONI SOCIALI

Il processo relativo alla gestione delle comunicazioni sociali è presidiato da un sistema di controlli basato sui seguenti principi:

- trasparenza;
- divieto di diffondere informazioni non chiare, non corrette, false e fuorvianti;
- divieto di diffondere informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti;
- divieto di omettere informazioni;
- divieto di produrre e diffondere materiale artefatto;
- implementazione di misure procedurali e organizzative per la prevenzione dei reati societari che possono essere commessi all'interno della Società;
- obbligo di attenersi alle procedure interne in materia di informativa periodica[5]; nello specifico, il riferimento è alle procedure che prevedono una rendicontazione periodica nei confronti del Consiglio di Amministrazione, ovvero, in particolare, quelle denominate "Parti correlate", "Processo di investimento gestioni patrimoniali", "Processo di investimento gestioni collettive", "Segreteria societaria", nonché la policy sui "Conflitti di interesse", quella in materia di "Remunerazione e incentivazione", "Antiriciclaggio" e i Regolamenti dei diversi Comitati esistenti;
- implementazione di sistemi di sicurezza logica e di altre procedure a garanzia della corretta gestione delle informazioni;
- obbligo del rispetto delle vigenti disposizioni in materia di bilancio e informativa nei confronti della clientela;
- regolamentazione dei poteri di firma;
- monitoraggio, a mezzo di controlli di primo e secondo livello, dei dati e delle informazioni oggetto di informativa (principio del "doppio controllo");
- monitoraggio da parte del Collegio Sindacale e della Società di Revisione dei dati e delle informazioni contenuti nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge.

7.3.3.3.1. GESTIONE DELLA LIQUIDITÀ SOCIETARIA

[5] Le procedure interne delineano il processo per la predisposizione dell'informativa periodica, nonché le funzioni aziendali responsabili del processo medesimo.

Il denaro contante (in euro e/o in valuta estera), presente in misura contenuta presso le casse della SGR, viene utilizzato per le "piccole spese" della segreteria quali, ad esempio, piccoli acquisti di cancelleria, materiale di consumo o altro, e donazioni di importo esiguo nel limite massimo di € 950,00. Esso può venire utilizzato, in misura molto limitata, per eventuali anticipi ai dipendenti che debbano effettuare trasferte di lavoro. Tali anticipi vengono corrisposti nel limite massimo di € 950,00, o importo equivalente in valuta estera. L'utilizzo del denaro contante da parte della segreteria viene accompagnato da apposito supporto documentale. L'eventuale utilizzo di contante come anticipo durante le trasferte viene riportato nelle note spese dei dipendenti. Non sono utilizzati titoli al portatore.

Gli assegni bancari vengono utilizzati, con scarsa frequenza, per pagare pochi specifici fornitori e per il prelievo del denaro contante tenuto presso la cassa della SGR. Di norma, non vengono, invece, utilizzati assegni circolari.

I pagamenti ai fornitori (esclusi quei pochi a cui si è fatto riferimento nella parte relativa ai pagamenti a mezzo assegno) vengono effettuati a mezzo bonifico bancario.

Gli ordini di pagamento possono essere in forma cartacea oppure mediante imputazione nel sistema di remote banking della banca dove viene tenuto il conto corrente dedicato ai pagamenti.

Gli ordini di pagamento in forma cartacea vengono predisposti mediante elaborazione di un foglio elettronico che riepiloga, per ogni fornitore:

- l'importo da pagare, tenuto conto di eventuali anticipi precedentemente pagati;
- l'IBAN;
- il numero identificativo delle fatture da pagare;
- la data valuta a favore dello stesso, se dovuta.

Una volta predisposti, gli ordini di bonifico vengono stampati su carta intestata e controllati nella loro correttezza dalla persona che li ha preparati. Successivamente, vengono controllati e siglati dall'Addetto senior ed infine firmati dalle persone all'uopo autorizzate e trasmessi alla banca affinchè venga processato il pagamento. Tali ordini di bonifico devono essere firmati secondo quanto previsto dalla procedura in materia di firme societarie. Dopo aver accertato, tramite home banking, l'avvenuto pagamento, questo viene contabilizzato e la fotocopia del bonifico viene archiviata in apposito raccoglitore.

I pagamenti eseguiti tramite sistema di remote banking vengono predisposti da un addetto dell'Unità Finanza, controllati da un addetto senior della stessa Unità che li valida e, infine, controllati e firmati elettronicamente dalle persone all'uopo autorizzate in ossequio alle previsioni contenute nella procedura in materia di firme societarie.I pagamenti infragruppo prevedono dei controlli incrociati tra l'Unità Analisi di Gestione e l'Unità Finanza. Annualmente, sulla base dei dati forniti dall'Unità Analisi di Gestione, viene effettuato uno scambio di corrispondenza tra le consociate, recante il dettaglio degli importi oggetto di fatturazione per le attività descritte nei documenti contrattuali che stabiliscono le varie tipologie di riaddebiti intragruppo. Con frequenza almeno annuale, o a cadenza diversa in funzione di particolari esigenze temporanee, si predispongono le fatture, si effettuano le registrazioni negli appositi conti di contabilità generale ed infine si provvede al relativo pagamento esclusivamente a mezzo bonifico bancario, seguendo la relativa procedura di effettuazione.

7.3.3.3.2. PREDISPOSIZIONE DEI PAGAMENTI

I pagamenti connessi allo svolgimento dell'attività societaria vengono predisposti dall'addetto dell'Unità Finanza che procede ad un controllo di primo livello su:

- correttezza dei dati inseriti o nei bonifici predisposti in forma cartacea o nei bonifici predisposti tramite sistema di remote banking;
- corrispondenza degli importi con le previsioni economiche dei contratti in essere e sulla base dei quali vengono pagati i costi ricorrenti;
- presenza, sulla fattura o sul documento fiscalmente valido equivalente, della sigla di approvazione del responsabile dell'unità a cui il costo è riferito, o, in alternativa, presenza di una e-mail autorizzativa della spesa, laddove il costo non sia previsto in un contratto sottoscritto dalla Società.

L'Addetto dell'Unità Finanza sottopone il bonifico all'attenzione dell'addetto senior, il quale, come controllo di secondo livello, verifica la congruità degli importi oggetto di bonifico e la ragionevolezza dei destinatari dei pagamenti, chiedendo, se del caso, ulteriori spiegazioni all'addetto che ha predisposto il pagamento. Infine, le disposizioni di pagamento vengono sottoposte alle persone all'uopo autorizzate per la firma manuale o digitale, nel rispetto delle modalità previste dalla procedura in materia di firme societarie.

Per quanto concerne i bonifici in forma cartacea, lla banca corrispondente garantisce il controllo di terzo livello sulla corretta applicazione dei limiti di spesa, in quanto in possesso non solo dello

specimen di firma, ma anche dei poteri delegati sulla base dei quali la banca è tenuta alle verifiche di correttezza, in applicazione delle disposizioni regolamentari specifiche del settore bancario in materia di esecuzione dei bonifici.

Al termine del processo, l'Addetto dell'Unità Finanza archivia copia dei bonifici, in ordine cronologico di registrazione, in apposito faldone tenuto presso l'Unità Finanza stessa.

Per quanto riguarda la determinazione ed il pagamento delle retrocessioni commissionali e delle commissioni di collocamento, l'Unità Analisi di Gestione procede trimestralmente al calcolo su base analitica degli importi dovuti alle diverse controparti in funzione del valore delle masse/delle quote possedute ogni fine mese da ciascuna controparte.

I suddetti calcoli, svolti su diversi file excel, una volta completati sono sintetizzati all'interno di un apposito report, inoltrato dall'Unità Analisi di Gestione al Direttore Finanza e Controllo per una verifica di coerenza e congruità di secondo livello.

Una volta validati i calcoli, l'Unità Analisi di Gestione archivia, in forma elettronica, una copia del file excel, contenente i calcoli effettuati, nonché l'evidenza della validazione da parte del Direttore Finanza e Controllo, comprovante l'avvenuto controllo di secondo livello.

L'Unità Analisi di Gestione trasmette, infine, le informazioni necessarie all'Addetto dell'Unità Finanza che provvede alla predisposizione dei bonifici sulla base dei dati ricevuti.

A predisposizione dei bonifici ultimata, il Responsabile dell'Unità Analisi di Gestione effettua un controllo di correttezza e completezza degli stessi prima di firmarli per l'invio alla banca corrispondente. Il controllo svolto dal Responsabile dell'Unità Analisi di Gestione ha ad oggetto l'importo e il destinatario del bonifico.

Copia del bonifico, con evidenza del controllo di secondo livello svolto (apposizione di segni di spunta sulle voci verificate), è archiviata a cura dell'Addetto dell'Unità Finanza.

Si rinvia a quanto sopra descritto in tema di bonifici per quanto concerne i successivi passaggi in materia di firme.

7.3.3.3.3. RICONCILIAZIONI BANCARIE

Le riconciliazioni sui conti correnti bancari utilizzati per lo svolgimento dell'attività societaria vengono predisposte dall'Addetto dell'Unità Finanza che procede ad un controllo di primo livello su:

- correttezza e completezza dei dati riportati nel prospetto di riconciliazione;
- congruità degli importi di spesa indicati nell'estratto conto bancario;

- completezza e ragionevolezza degli importi in riconciliazione tra l'estratto conto bancario e le evidenze contabili.

L'Addetto dell'Unità Finanza, previa apposizione della propria sigla sui prospetti di riconciliazione, attestante gli avvenuti controlli sopra descritti, trasmette su base periodica tali prospetti all'addetto senior dell'Unità stessa.
L'addetto senior dell'Unità Finanza, quale controllo di secondo livello, verifica la corrispondenza dei saldi riportati nei prospetti di riconciliazione con i saldi indicati negli estratti conto bancari, unitamente ad altri controlli quali, a titolo esemplificativo e non esaustivo, la congruità degli importi in riconciliazione e l'ageing degli importi in riconciliazione, chiedendo le opportune delucidazioni all'Addetto dell'Unità Finanza, laddove opportuno.
Al termine del controllo, l'addetto senior appone la propria sigla sul prospetto cartaceo, quale evidenza della avvenuta effettuazione del controllo stesso.

Al termine del processo, l'Addetto dell'Unità Finanza archivia i prospetti delle riconciliazioni bancarie suddivisi per banca controparte ed in ordine cronologico in apposito faldone tenuto presso l'Unità stessa.

I prospetti delle riconciliazioni bancarie sono oggetto di un terzo livello di controllo da parte del Responsabile dell'Unità Internal Audit, il quale – sulla base del proprio piano annuale dei controlli – esegue le opportune verifiche.

Un quarto livello di controllo è, infine, garantito dalle verifiche effettuate dalla Società di Revisione nell'ambito delle proprie procedure finalizzate all'emissione della relazione di certificazione del Bilancio.

7.3.3.4. CHIUSURA DELLA CONTABILITÀ GENERALE

7.3.3.4.1. REGISTRAZIONE DEGLI ACCERTAMENTI ATTIVI E PASSIVI, RATEI E RISCONTI

In sede di predisposizione del Bilancio annuale, gli Addetti dell'Unità Finanza, ognuno per la propria competenza e responsabilità, sotto la supervisione del più senior, provvedono alla compilazione di apposito prospetto excel, che accorpa tutti i dati extracontabili relativi agli accertamenti attivi e passivi, ai ratei ed ai risconti.
La determinazione degli accertamenti (ad esempio delle fatture da ricevere) avviene, non solo sulla base delle informazioni disponibili e dei colloqui con i Responsabili dell'Unità Finanza e dell'Unità

Analisi di Gestione, ma anche sulla base di specifiche richieste inoltrate alle controparti, allo scopo di verificare che non vi siano pendenze non prese in considerazione per la completa e corretta appostazione degli accertamenti stessi.

La determinazione dei ratei e dei risconti avviene sulla base dell'analisi delle evidenze documentali, quali i contratti in essere, ove presenti, in funzione delle quali viene determinata la corretta competenza dei relativi costi/ricavi, allo scopo di effettuare le opportune rettifiche, in aumento o in diminuzione, mediante lo strumento dei ratei e dei risconti.

Le suddette attività vengono dapprima controllate dall'Addetto dell'Unità Finanza che le ha svolte (primo livello); quindi, dall'Addetto senior dell'Unità stessa (secondo livello); e infine, dall'Unità Analisi di Gestione, che svolge un'analisi di coerenza e congruità degli importi (terzo livello).

Il controllo di quarto livello viene garantito dalle verifiche effettuate dalla Società di Revisione nell'ambito delle proprie procedure finalizzate all'emissione della relazione di certificazione del Bilancio.

Al termine del processo, i prospetti utilizzati per la determinazione degli accertamenti, e controllati dall'Unità Finanza, sono archiviati in formato elettronico in una directory condivisa nell'ambito dell'Unità Finanza stessa.

Per quanto concerne i saldi dei rapporti intragruppo, l'Unità Analisi di Gestione predispone ed aggiorna su base mensile un apposito file in formato elettronico, che ricomprende tutti gli accertamenti – dell'anno di riferimento – di natura economica derivanti dalle relazioni intragruppo, e comunica le risultanze all'Addetto dell'Unità Finanza, per il corretto e completo recepimento di tali saldi negli aggiustamenti extracontabili dei saldi mensili.

In sede di chiusura dell'esercizio, l'operazione ora descritta è sottoposta a un controllo generale di tutte le partite aperte, della movimentazione dell'anno oggetto di Bilancio e delle partite ancora da appostare, per rendere una corretta evidenza dei saldi intragruppo alla data di chiusura del Bilancio.

Il citato controllo è svolto, al primo livello, dagli addetti dell'Unità Finanza e, al secondo livello, dall'Unità Analisi di Gestione.

In questa fase viene coinvolto anche il Responsabile dell'Unità Finanza per un suo controllo ulteriore di coerenza e congruità dei saldi da indicare in Bilancio (controllo di terzo livello).

In ultima istanza, la correttezza e completezza delle poste intragruppo viene assoggettata a controllo da parte della Società di Revisione nell'ambito delle proprie procedure finalizzate all'emissione della relazione di certificazione del Bilancio.

Al termine del processo, il Responsabile dell'Unità Analisi di Gestione archivia in formato elettronico il file sopra menzionato, utilizzato per la determinazione dei saldi intragruppo, in una specifica directory.

Sempre in formato elettronico, il Responsabile dell'Unità Analisi di Gestione:

- lascia traccia del controllo svolto;
- appone la propria sigla sulla copia del file sopra citato;
- provvede alla sua archiviazione.

Gli addetti dell'Unità Finanza provvedono, infine, ad archiviare in formato elettronico il file ricevuto dall'Unità Analisi di Gestione in una directory condivisa dell'Unità Finanza.

7.3.3.4.2. DETERMINAZIONE DELLE POSTE DI STIMA

In sede di predisposizione del Bilancio annuale, gli addetti dell'Unità Finanza, il Responsabile dell'Unità Finanza e il Responsabile dell'Unità Analisi di Gestione, ognuno per le parti di propria competenza e responsabilità, ed i primi sotto la supervisione del secondo, provvedono all'identificazione delle eventuali poste di stima, e alla corretta determinazione dell'importo dell'accantonamento.

Per lo svolgimento delle attività ora descritte, i soggetti citati si basano su tutte le informazioni disponibili, nonché sui risultati delle valutazioni effettuate con l'Amministratore Delegato, laddove le eventuali poste di stima siano di notevole rilevanza per importo o per complessità.

Nel caso di poste di stima previste dai principi contabili applicabili, quale, a titolo esemplificativo, il valore attuariale del fondo TFR da appostare in Bilancio, gli addetti dell'Unità Finanza si avvalgono del supporto di consulenti specializzati in materia.

I risultati delle valutazioni effettuate dagli addetti dell'Unità Finanza e dai consulenti coinvolti vengono rivisti con il Responsabile dell'Unità Finanza che, nello svolgimento dei propri controlli di secondo livello, valuta anche la congruità e la ragionevolezza degli assunti alla base delle elaborazioni, unitamente alla correttezza dei risultati conseguiti. Con riferimento, a titolo esemplificativo, alla determinazione del fondo TFR, il Responsabile dell'Unità Finanza verifica con l'Alta Direzione le dinamiche retributive prospettiche e le previsioni di assunzioni future. Tali elementi, che vengono utilizzati dal consulente esterno per modellizzare il prospetto di calcolo dell'attualizzazione del valore del fondo TFR, vengono indicati espressamente nella relazione accompagnatoria, nella quale sono descritti non solo i presupposti, ma anche le conclusioni tratte sulla base di questi ultimi. Il Responsabile dell'Unità Finanza rivede e valida gli assunti e le conclusioni. La relazione è archiviata a cura degli addetti dell'Unità Finanza.

Laddove la particolarità della valutazione da effettuare e/o la rilevanza economica dell'appostazione di un eventuale fondo rischi ed oneri e/o altra posta di stima lo richieda/richiedano, il Responsabile dell'Unità Finanza e il Direttore Finanza e Controllo coinvolgono nel processo la Società di Revisione, al fine di ottenere un conforto sul corretto trattamento dell'evento oggetto di disamina e sulla corretta determinazione dell'appostazione in contabilità generale. Nella fattispecie, viene coinvolto anche il Collegio Sindacale, affinché lo stesso possa esprimere le proprie considerazioni in merito alla correttezza dell'approccio adottato ed alla congruità dei risultati cui si è pervenuti.
In ultima istanza, la correttezza delle poste di stima viene assoggettata a controllo da parte della Società di Revisione, nell'ambito delle proprie procedure finalizzate all'emissione della relazione di certificazione del Bilancio.

7.3.3.4.3. DETERMINAZIONE DEL FONDO IMPOSTE

In sede di predisposizione del Bilancio annuale, gli addetti dell'Unità Finanza trasmettono apposito file excel, riportante la situazione contabile finale (dati contabili ed extra-contabili), al consulente fiscale affinché questi provveda alla determinazione:

- delle imposte, a carico della Società, di competenza dell'esercizio di riferimento;
- delle imposte anticipate e differite, con i relativi impatti a conto economico, aventi il fine di neutralizzare gli effetti delle "timing differences" dovute all'applicazione di criteri di determinazione dell'utile imponibile diversi rispetto ai criteri civilistici di determinazione del Bilancio e dell'utile d'esercizio.

Una volta determinate le varie componenti patrimoniali ed economiche riferite alle imposte, il consulente fiscale fornisce agli addetti dell'Unità Finanza un prospetto, in formato excel, affinché questi ultimi possano effettuare i propri controlli, di secondo livello, sulla correttezza e completezza dei dati utilizzati dal consulente fiscale stesso, nella determinazione delle imposte cui la Società è assoggettata e di quelle anticipate e differite.
Il Responsabile dell'Unità Finanza esegue un controllo di terzo livello sulla congruità degli assunti alla base della determinazione dei gravami di imposta e sulle voci maggiormente peculiari e/o di più difficile interpretazione o valutazione.
Il prospetto controllato dall'Unità Finanza è archiviato in formato elettronico a cura dell'Unità stessa.

In ultima istanza, la correttezza delle voci riferite al fondo imposte ed ai crediti e debiti per imposte anticipate e differite viene assoggettata a controllo da parte della Società di Revisione, nell'ambito delle proprie procedure finalizzate all'emissione della relazione di certificazione del Bilancio.

7.3.3.5. REDAZIONE ED APPROVAZIONE DEL BILANCIO D'ESERCIZIO

7.3.3.5.1. REDAZIONE DEL BILANCIO D'ESERCIZIO

Una volta completata la predisposizione dei dati a supporto della redazione dei documenti di Bilancio, come descritto nelle precedenti sezioni, gli addetti dell'Unità Finanza predispongono i dati per la compilazione del Bilancio annuale, secondo i principi contabili internazionali applicabili (IAS/IFRS).

Tale attività è svolta mediante il sopracitato file excel.
Partendo dai saldi della contabilità generale e aggiungendovi tutte le voci di accertamento e di rettifica, gli addetti dell'Unità Finanza giunge alla determinazione dei saldi di Bilancio.
Gli addetti dell'Unità Finanza utilizzano il citato file per la compilazione degli schemi di Bilancio e la predisposizione degli schemi di dettaglio da indicare in Nota Integrativa.
Laddove servissero ulteriori dettagli da riportare in Nota Integrativa, gli addetti dell'Unità Finanza:

- esaminano le schede contabili e/o le scritture contabili nel sistema di contabilità generale;
- nel caso in cui i riferimenti siano ai saldi intragruppo e/o ai costi e ricavi legati alle commissioni passive e attive, controllano i dettagli predisposti con il Responsabile dell'Unità Analisi di Gestione;
- nel caso in cui i riferimenti siano relativi ai saldi delle imposte dell'esercizio, viene coinvolto il consulente fiscale;
- per quanto concerne informazioni di natura qualitativa più complesse e/o articolate, viene coinvolto il Responsabile dell'Unità Finanza, che procede alla stesura delle note esplicative da riportare in Nota Integrativa.

Gli addetti dell'Unità Finanza, nella redazione degli schemi di Bilancio e delle tabelle di dettaglio di Nota Integrativa, effettuano un controllo di primo livello verificando la corrispondenza fra il file sopracitato e le risultanze contabili, nonché la quadratura degli importi sia nelle singole tabelle sia tra tabelle collegate.

L'addetto senior dell'Unità Finanza predispone la tabella del Rendiconto Finanziario sulla base dei seguenti schemi di Bilancio d'Esercizio e delle seguenti schede contabili:

- dettaglio delle immobilizzazioni immateriali;
- dettaglio dei ratei e risconti attivi e passivi;
- dettaglio dei dati fiscali e dei pagamenti intervenuti nel corso dell'esercizio;
- dettaglio dei movimenti dei fondi e delle altre attività e passività;
- dettaglio del fondo TFR e dei relativi movimenti.

L'addetto senior dell'Unità Finanza predispone il prospetto delle Variazioni di Patrimonio Netto sulla base delle delibere assembleari di riferimento, delle schede contabili dei movimenti delle voci che compongono il patrimonio netto e di eventuale ulteriore documentazione a supporto.

L'addetto senior dell'Unità Finanza predispone il prospetto della Redditività Complessiva, dove viene esposta la redditività complessiva prodotta, partendo dal risultato d'esercizio e scorporando l'effetto dovuto all'applicazione dei principi contabili IAS su alcune componenti delle attività e delle passività di Bilancio.

L'addetto senior dell'Unità Finanza effettua il controllo di secondo livello su tutta la documentazione di Bilancio predisposta dall'altro addetto della medesima Unità (schemi, Nota Integrativa, Prospetti).
Il Responsabile dell'Unità Finanza esegue il controllo di terzo livello rivedendo, a sua volta, le parti salienti della documentazione di Bilancio.
In ultima istanza, la correttezza e la completezza delle informazioni riportate nel documento di Bilancio, così come la loro corrispondenza a quanto indicato nella contabilità generale e la coerenza con quanto indicato nella Relazione sulla Gestione, vengono assoggettate a controllo da parte della Società di Revisione, nell'ambito delle proprie procedure finalizzate all'emissione della relazione di certificazione del Bilancio.

La documentazione prodotta dagli addetti dell'Unità Finanza (schemi, Nota Integrativa, Prospetti), e controllata, è archiviata in formato cartaceo e\o elettronico a cura della medesima Unità.

La Relazione sulla Gestione viene predisposta a più mani, a seconda delle conoscenze e competenze delle persone coinvolte.

Il Responsabile dell'Unità Finanza interviene per le parti di propria competenza in merito ai commenti sui dati di Bilancio, sui dati relativi ai movimenti del personale ed alle altre informazioni di carattere societario.
Il Responsabile dell'Unità Analisi di Gestione interviene sulle parti descrittive relative alla redditività e alle masse dei vari prodotti gestiti dalla Società.
Il Responsabile dell'Unità Rapporti con le Autorità di Vigilanza predispone la parte dedicata agli eventi di natura regolamentare intervenuti nel corso dell'anno, quali modifiche dei prospetti informativi dei fondi gestiti dalla Società.
L'Amministratore Delegato predispone i commenti al mercato, quelli sull'andamento societario nel corso dell'esercizio oggetto di Bilancio, nonché sulle previsioni prospettiche.
Il coordinamento della redazione della Relazione sulla Gestione e la verifica che tutte le parti di competenza di ognuno siano state predisposte ricadono in capo all'Addetto dell'Unità Affari Legali e Societari.
Quest'ultimo provvede a raccogliere, sulle parti di Relazione sulla Gestione di competenza, la sigla dei diversi soggetti coinvolti, ovvero del Responsabile dell'Unità Finanza, del Responsabile dell'Unità Analisi di Gestione e del Responsabile dell'Unità Rapporti con le Autorità di Vigilanza.

Il documento completo, datato e siglato dall'Amministratore Delegato, è archiviato in forma cartacea a cura dell'Addetto dell'Unità Affari Legali e Societari.

7.3.3.5.2. APPROVAZIONE DEL BILANCIO D'ESERCIZIO

Adottando lo stesso criterio descritto in precedenza a proposito della predisposizione della Relazione sulla Gestione, la parte del verbale del Consiglio di Amministrazione propedeutica all'approvazione della bozza di Bilancio, da sottoporre all'Assemblea, è predisposta a più mani dai vari responsabili di unità, ciascuno per le proprie aree di competenza. Il coordinamento di questa fase procedurale viene effettuato dal Responsabile dell'Unità Affari Legali e Societari, che si occupa di conservare elettronicamente le parti di verbale predisposte dai diversi soggetti coinvolti.

La bozza di Bilancio discussa in sede di Consiglio di Amministrazione è oggetto di controllo anche da parte della Società di Revisione, nell'ambito dell'iter finalizzato al rilascio, nei tempi previsti, della relazione di certificazione (prima dell'Assemblea dei Soci).
Una volta approvata la bozza di Bilancio dal Consiglio di Amministrazione della Società, questa é depositata presso la sede sociale nei tempi previsti dalla normativa vigente, e successivamente é

sottoposta all'Assemblea dei Soci, che ne delibera l'approvazione, e che, unitamente, delibera in merito alla destinazione dell'utile d'esercizio e alla movimentazione delle riserve, tenendo in considerazione la proposta ricevuta dal Consiglio di Amministrazione.

Delle delibere assembleari viene redatto apposito verbale dei cui contenuti il Responsabile dell'Unità Finanza porta a conoscenza gli addetti dell'Unità stessa, affinché si proceda alla rilevazione delle adeguate registrazioni contabili nel sistema di contabilità generale.

Il Responsabile dell'Unità Finanza verifica la corretta registrazione della destinazione dell'utile d'esercizio e dei movimenti delle riserve di patrimonio, sulla base di quanto deliberato in sede assembleare.

Il Responsabile dell'Unità Rapporti con le Autorità di Vigilanza si occupa della trasmissione del Bilancio a Banca d'Italia (per l'inoltro a Consob, cfr. "Elaborazione e trasmissione delle segnalazioni"), e al deposito in Camera di Commercio, nei tempi e nei modi previsti dalla normativa applicabile.

Annualmente, il Responsabile dell'Unità Compliance verifica l'invio del Bilancio alle AA.VV., mediante controllo dell'evidenza del corretto trasferimento dei dati.

7.3.3.6. GESTIONE ACCESSI SISTEMI/APPLICATIVI

Il personale dipendente della Società ha accesso al sistema ed alla rete solo mediante utilizzo di "userID" e "password". Ogni dipendente, in funzione del ruolo svolto all'interno della Società, ha accesso solo a specifiche directory ed applicativi.

Una volta entrati nel sistema principale, l'accesso a quello della contabilità generale è consentito solo all'Unità Finanza e all'Unità Analisi di Gestione.

Ognuno è censito nel sistema con un'utenza individuale e nominativa; per entrarvi è necessario inserire il proprio "userID" (specifico del sistema di contabilità generale) ed una "password".

Il sistema di contabilità generale è di proprietà di un provider terzo, Xchanging Italy S.p.A., che ha accesso al sistema proprietario mediante utilizzo di "userID" e "password", così come avviene all'interno della Società.

Nel rispetto delle previsioni normative sulla privacy, sia gli accessi al sistema in Società sia gli accessi al sistema in Xchanging Italy S.p.A. sono assoggettati a modalità di registrazione, al fine di individuare eventuali violazioni dei livelli ed autorizzazioni agli accessi, oppure eventuali violazioni commesse dai dipendenti una volta entrati nel sistema.

Il Responsabile dell'Unità IT ha il compito di attribuire i differenti livelli di accesso in funzione delle indicazioni fornite dal responsabile dell'unità cui il dipendente appartiene, e di monitorare il corretto utilizzo dei sistemi informatici in uso ai dipendenti della Società.

Accanto al sistema di contabilità generale di proprietà di Xchanging Italy S.p.A., il Responsabile dell'Unità Analisi di Gestione utilizza e manutiene un "database", nel quale sono riportati, anno per anno, i dati retributivi del personale della Società (parte fissa e parte variabile della retribuzione).

Trattasi di "database" coperto da password, al quale può accedere solo il Responsabile dell'Unità Analisi di Gestione.

7.3.3.7. PREDISPOSIZIONE DEI PROSPETTI INFORMATIVI E DEI REGOLAMENTI DI GESTIONE

Il processo relativo alla predisposizione dei prospetti informativi e dei regolamenti di gestione è presidiato da un sistema di controlli basato sui seguenti principi:

- trasparenza;
- divieto di diffondere informazioni non chiare, non corrette, false e fuorvianti;
- divieto di diffondere informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti;
- divieto di omettere informazioni;
- divieto di produrre e diffondere materiale artefatto;
- implementazione di misure procedurali e organizzative per la prevenzione dei reati societari che possono essere commessi all'interno della Società;
- obbligo di attenersi alle procedure interne in materia di informativa periodica[6];
- implementazione di sistemi di sicurezza logica e di altre procedure a garanzia della corretta gestione delle informazioni;
- obbligo del rispetto delle vigenti disposizioni in materia di bilancio e informativa nei confronti della clientela;
- regolamentazione dei poteri di firma;
- monitoraggio, a mezzo di controlli di primo e secondo livello, dei dati e delle informazioni oggetto di informativa (principio del "doppio controllo");

[6] Le procedure interne delineano il processo per la predisposizione dell'informativa periodica, nonché le funzioni aziendali responsabili del processo medesimo.

- monitoraggio da parte del Collegio Sindacale e della Società di Revisione dei dati e delle informazioni contenuti nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge.

L'iter procedurale previsto all'interno della SGR per la regolamentazione del processo relativo alla predisposizione dei prospetti informativi degli OICR domestici e dei regolamenti di gestione è basato sui seguenti presidi:

- definizione di un'apposita unità, l'Unità Rapporti con le AA.VV., dedicata fra l'altro alla redazione dei prospetti informativi e dei regolamenti di gestione;
- predisposizione, da parte di ogni soggetto competente (Unità Compliance, Unità Risk Management, Unità Operations, Unità Affari Legali e Societari e Unità Rapporti con le AA.VV.), dei dati/documentazione/parti di prospetto o regolamento di gestione necessari alla redazione del documento finale;
- apposizione di data e sigla da parte del soggetto competente sui dati/documentazione/parti di prospetto o regolamento di gestione predisposti per la redazione del documento finale;
- il prospetto informativo e il testo regolamentare sono sempre sottoposti al vaglio del Responsabile dell'Unità Compliance, il quale ne verifica la congruenza con la normativa di riferimento al momento in vigore, e fornisce il proprio parere a mezzo email;
- il prospetto informativo, da inoltrare all'Autorità di Vigilanza competente, è siglato\firmato dal Responsabile dell'Unità Rapporti con le AA.VV., che ha sovrinteso alla relativa redazione, previo parere favorevole di congruenza con la normativa di riferimento fornito dal Responsabile dell'Unità Compliance, nel rispetto del principio del doppio controllo;
- la "scheda di deposito", da inoltrare all'Autorità di Vigilanza unitamente al prospetto informativo, è predisposta e inviata dallo studio legale esterno investito dell'incarico di inoltro del prospetto stesso, secondo le vigenti procedure Consob, previa verifica del Responsabile dell'Unità Rapporti con le AA.VV.;
- il regolamento di gestione, da inoltrare all'Autorità di Vigilanza competente, è trasmesso al Responsabile dell'Unità Rapporti con le AA.VV. dal Responsabile dell'Unità Affari Legali e Societari, corredato dal relativo estratto del verbale consiliare e siglato;
- tutti i dati e la documentazione forniti per la redazione del prospetto informativo e del regolamento di gestione, unitamente al prospetto informativo e al regolamento di gestione inviati, sono archiviati a cura dell'Unità Rapporti con le AA.VV.

L'iter procedurale previsto all'interno della SGR per la regolamentazione del processo relativo alla predisposizione dei prospetti informativi degli OICR di diritto lussemburghese istituiti dalla Società è basato sui seguenti presidi:

- definizione di un'apposita unità, l'Unità Progetti Speciali, dedicata al coordinamento della predisposizione dei prospetti informativi degli OICR di diritto lussemburghese istituiti dalla Società, in collaborazione con i Consigli di Amministrazione degli OICR stessi, i consulenti legali e le funzioni aziendali rilevanti;
- predisposizione, da parte dell'Unità Progetti Speciali, della bozza di prospetto informativo, da sottoporre alla revisione delle funzioni aziendali competenti (ad es. Unità Compliance, Unità Risk Management, Unità Operations e Unità Investimenti Gestioni Collettive) in conformità con le delibere del Consiglio di Amministrazione della Società e del Consiglio di Amministrazione dell'OICR interessato;
- circolarizzazione della bozza per eventuali commenti, ove rilevanti, prima dell'invio all'Autorità di Vigilanza lussemburghese;
- il prospetto informativo è inoltrato all'Autorità di Vigilanza lussemburghese a cura dei consulenti legali;
- i consulenti legali curano i rapporti con l'Autorità di Vigilanza, ricevendone le eventuali richieste di chiarimenti e trasmettendo alla stessa le risposte fornite dalla SGR;
- l'Unità Progetti Speciali riceve gli eventuali commenti dell'Autorità di Vigilanza (tramite i legali) e coordina l'invio delle risposte eventualmente con l'assistenza delle funzioni aziendali competenti;
- una volta ottenuta l'approvazione verbale del prospetto informativo da parte dell'Autorità di Vigilanza lussemburghese, i consulenti legali forniscono la versione finale, che sottopongono alla procedura di visa (approvazione ufficiale apposta con firma elettronica dall'Autorità di Vigilanza);
- l'Unità Progetti Speciali coordina le procedure per la commercializzazione cross border degli OICR esteri, incluse l'eventuale traduzione del Prospetto in lingue diverse dalla lingua inglese, nonché la predisposizione, da parte del fornitore all'uopo identificato, dei KIID in lingua inglese e nelle lingue dei paesi dove gli OICR di diritto lussemburghese istituiti dalla Società saranno distribuiti;

- l'Unità Progetti Speciali coordina, inoltre, attraverso i consulenti scelti dalla SGR, la trasmissione della documentazione aggiornata alle Autorità di Vigilanza dei paesi dove gli OICR di diritto lussemburghese istituiti dalla Società saranno distribuiti.

7.3.3.8 RAPPORTI NEGOZIALI CON INVESTITORI ED ENTI PRIVATI

Tutti i rapporti negoziali con soggetti privati – investitori, banche, assicurazioni, fornitori di beni e servizi, consulenti, etc. – sono tenuti nel rispetto dei seguenti principi di controllo e di comportamento:

- divieto di effettuare/promettere elargizioni in denaro, o accordare/promettere vantaggi di qualsiasi natura (ad esempio: promesse di assunzioni, di accordi strategici finanziari etc.) ad esponenti - apicali o sottoposti – di altre società private, strumentali ad ottenere vantaggi per la Società (in termini economici, conoscitivi, strategici etc.) che non rientrino nella normale e trasparente pratica degli affari;
- in particolare, nell'ambito dei rapporti con enti investitori o potenziali tali, nonché con enti bancari e creditizi, agli operatori della Società è fatto divieto di promettere (o corrispondere) ad esponenti aziendali di tali enti qualsivoglia vantaggio personale, diretto o indiretto, come corrispettivo per determinare o agevolare la decisione di investimento all'interno della Società o per determinare o agevolare la concessione di finanziamenti, prestiti, crediti, garanzie a favore della Società;
- nell'ambito di incontri, professionali e non, o comunque di comunicazioni con esponenti aziendali di altre società commerciali, nonché di incontri o di comunicazioni con giornalisti della stampa e dell'informazione economico-finanziaria, è fatto divieto agli operatori della Società di dare o promettere qualsivoglia vantaggio personale ai soggetti privati al fine di ottenere la rivelazione di informazioni privilegiate o al fine di indurre i giornalisti alla pubblicazione di informazioni privilegiate, false o fuorvianti, idonee ad alterare il prezzo di strumenti finanziari nell'interesse, diretto o indiretto, della Società;
- divieto di determinare compensi, effettuare prestazioni o accordare, direttamente o indirettamente, benefici di qualsiasi natura in favore di esponenti di partner o controparti commerciali o consulenti professionali che non trovino adeguata e comprovabile giustificazione nel contesto del rapporto costituito con gli stessi;
- divieto di concedere omaggi o regalie di qualunque genere di valore superiore alla normali pratiche di cortesia nei confronti di esponenti di altre società private che intrattengono e possano intrattenere rapporti finanziari, commerciali, consulenziali con la Società; in ogni

caso, le spese per regali, omaggi, offerta di servizi nei confronti dei suddetti soggetti privati, devono essere specificamente comunicate e registrate in quanto tali.

Al fine di minimizzare il rischio di condotte di corruzione tra privati assume particolare rilevanza l'organizzazione e il controllo sulle attività strumentali alla commissione di tali illeciti (ad esempio, attraverso la predisposizione di fondi occulti destinati alla remunerazione indebita del privato corrotto); in particolare:

- selezione e gestione di contratti di consulenza e di outsourcing;
- selezione, remunerazione e incentivazione del personale;
- gestione della finanza, della tesoreria, della contabilità generale e del bilancio;
- gestione di omaggi, regali, spese di rappresentanza e sponsorizzazioni.

Al riguardo, è fatto obbligo di osservare le regole di condotta, i protocolli comportamentali e la filiera dei controlli formalizzati nel Modello (in particolare, nella presente sezione, relativa ai reati societari, nonché nella sezione relativa ai reati contro la Pubblica Amministrazione) e nel "Manuale delle procedure aziendali", le cui prescrizioni si intendono qui richiamate e costituiscono parte integrante del presidi di controllo e dei principi di comportamento anche nell'ottica della prevenzione delle condotte di corruzione tra privati.

7.4. DELITTI DI CRIMINALITÀ ORGANIZZATA, CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO E REATI TRANSNAZIONALI

Attraverso ripetuti interventi legislativi sono state introdotte nel sistema della responsabilità amministrativa degli Enti varie categorie di illeciti, con la comune finalità di contrastare fenomeni di criminalità che destano particolare allarme a livello internazionale, specie in relazione a reati di matrice politico-terroristica, oppure commessi nei settori e con le forme tipiche della delinquenza organizzata, anche transnazionale, o particolarmente lesivi di fondamentali diritti umani.

Il settore finanziario ha da sempre dedicato particolare attenzione ed impegno nella collaborazione alla prevenzione di fenomeni criminali nel mercato finanziario ed al contrasto al terrorismo, impegno che la SGR assume anche ai fini della tutela della sana e prudente gestione, della trasparenza e correttezza dei comportamenti, del buon funzionamento del sistema nel suo complesso, dell'applicazione rigorosa dei presidi AML in relazione alla propria clientela.

Alla luce dell'attività svolta dalla Società e al contesto in cui opera, risulta ovvio che le categorie di reato oggetto della presente Parte Speciale esprimono un rischio potenziale non tanto quali reati commessi in via diretta dagli esponenti dell'Ente, nel suo interesse, quanto piuttosto quali reati commessi da clienti (appartenti ad associazioni criminali) della Società che potrebbero trovare un beneficio o un supporto, soprattutto di natura economica, dall'attività di investimento prestata dalla Società per loro conto.

Su un altro versante, i reati di criminalità organizzata di cui all'art. 24-quater D.Lgs 231/01 (in particolare il reato di associazione per delinquere ex art. 416 c.p.), secondo un orientamento giurisprudenziale che sta ricevendo un seguito non insignificante, possono rappresentare, se commessi all'interno dell'ente, uno strumento di estensione, seppur indiretta, della responsabilità da "colpa di organizzazione" dell'Ente connessa alla mancata adozione di specifici presidi volti a prevenire la commissione dei reati fine dell'associazione, ancorchè si tratti di reati non compresi nel catologo dei reati presupposto ex D.Lgs 231/01. Tra questi, secondo quanto emerso dal Risk Assessment, potrebbero venire in rilievo – per ciò che attiene all'attività svolta dalla Società – alcuni illeciti fiscali (principalmente i delitti di cui agli artt. 4, 5 e 10 quater D.Lgs 74/20000) nella loro forma "classica" attualmente esclusa dal comma 1-bis dell'art. 25-quinquiesdecies D.Lgs 231/01, nonché alcuni reati contro il patrimonio (in particolare, il reato di truffa ex art. 640 c.p. a danno di clienti/investitori privati della Società, ossia un'ipotesi non rientrante tra i "reato presupposto 231").

In questa prospettiva, ne deriva un parziale ampliamento delle attività aziendali potenzialmente esposte ai rischi reato associativi e un corrispondente ampliamento dei connessi presidi, volti a prevenire non solo il reato associativo ma anche i suoi reati fine; tali presidi sono specificamente previsti, rispettivamente, nella Parte Speciale dedicata ai reati tributari e nella Parte Speciale dedicata ai reati contro l'industria ed il commercio, a cui si rinvia.

7.4.1. Fattispecie delittuose

Reati presupposto dell'illecito amministrativo di cui all'art. 24-quater D.Lgs. 231/01 emersi come potenzialmente rilevanti per la Società all'esito del Risk Assessment

Delitti di criminalità organizzata

L'art. 24-ter del Decreto, inserito dalla L. n. 94/2009, prevede innanzitutto un gruppo di reati inerenti alle varie forme di associazioni criminose, e cioè:

- Associazione per delinquere generica (art. 416 c.p., primi cinque commi);
- Associazione di tipo mafioso, anche straniera e scambio elettorale politico-mafioso (artt. 416-bis e 416-ter);
- Associazione per delinquere finalizzata alla commissione di delitti in tema di schiavitù, di tratta di persone e di immigrazione clandestina (art. 416 c.p., comma 6);
- Associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/1990).

Nella specifica prospettiva dei possibili rischi per la Società, rileva soprattutto la fattispecie associativa generica (art. 416 c.p.), che punisce il semplice fatto di associarsi, in tre o più persone, allo scopo di commettere più delitti (di qualsiasi tipologia).

Partecipa all'associazione, peraltro, colui che vi esplichi qualsiasi attività, ancorché secondaria; ed è proprio in tale vincolo associativo, dotato di permanenza o almeno di stabilità – oltre che nel numero minimo di tre associati e nell'indeterminatezza del programma criminoso – che vengono identificati i requisiti caratterizzanti dell'associazione a delinquere e a differenziarla dall'ipotesi del mero concorso nel reato (c.d. "concorso esterno").

La peculiarità dell'associazione di tipo mafioso (art. 416-bis c.p.) sta nell'utilizzo del "metodo mafioso", che si realizza "quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo

associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri".

Assume inoltre rilevanza, ai fini della responsabilità dell'Ente, qualsiasi fattispecie delittuosa che comunque venga realizzata avvalendosi del suddetto "metodo mafioso": cioè allorquando il soggetto agente, pur senza appartenere al sodalizio criminoso o concorrere con esso, pone in essere una condotta idonea ad esercitare una particolare intimidazione (ad esempio una richiesta nei confronti di una controparte, pubblica o privata) avvalendosi dello sfruttamento della "fama" di organizzazioni criminali operanti nell'ambito di un determinato territorio.

Infine, ai sensi dell'art. 24-ter, rilevano anche tutte le condotte illecite che, sebbene autonomamente non previste quali reati-presupposto ai fini dell'applicazione del Decreto, siano poste in essere allo scopo di agevolare l'attività di un'associazione di tipo mafioso (ad esempio il concorso nella commissione di un reato tributario o di una truffa finanziaria essendo a conoscenza della riferibilità dell'operazione ad una associazione mafiosa).

Va in ogni caso ricordato che, affinché sussista la possibilità di imputare l'illecito all'ente, è necessario che il reato sia stato commesso nell'interesse o a vantaggio dello stesso e non semplicemente avvalendosi della sua struttura per il perseguimento di un profitto riferibile esclusivamente al soggetto attivo.

Reati presupposto dell'illecito amministrativo di cui all'art. 25-quater D.Lgs. 231/01 emersi come potenzialmente rilevanti per la Società all'esito del Risk Assessment

Delitti con finalità di terrorismo o di eversione dell'ordine democratico L'art. 25-quater del Decreto dispone la punibilità dell'ente, ove ne sussistano i presupposti, nel caso in cui siano commessi, nell'interesse o a vantaggio dell'ente stesso, delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale, dalle leggi speciali o in violazione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9.12.1999. La norma non prevede un elenco di reati chiuso e tassativo, ma si riferisce ad un qualsivoglia illecito penale caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico perseguita dal soggetto agente.

Reati presupposto dell'illecito amministrativo di cui alla L. 146/2006 potenzialmente rilevanti per la Società all'esito del Risk Assessment

Reati transnazionali

La legge 16 marzo 2006, n. 146, entrata in vigore il 12 aprile 2006, nel dare attuazione all'art. 10 della "Convenzione delle Nazioni Unite contro il crimine organizzato transnazionale" (c.d. Convenzione di Palermo), adottata dall'Assemblea Generale il 15 novembre 2000 ed il 31 maggio 2001, ha esteso l'applicazione delle disposizioni di cui al Decreto anche ai cosiddetti "reati transnazionali".

L'art. 3 della citata legge definisce il "reato transnazionale" – un inedito per il nostro sistema penale – come il reato, punito con la pena della reclusione non inferiore nel massimo a quattro anni, che veda coinvolto un gruppo criminale organizzato e che, alternativamente:

- sia commesso in più di uno Stato;
- sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Il legislatore, tuttavia, prende in considerazione – quali reati-presupposto della responsabilità dell'Ente – una cerchia ristretta di fattispecie delittuose, che possono dividersi in quattro insiemi tipologici:

- reati di associazione per delinquere, associazione di tipo mafioso, associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri, associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope;
- riciclaggio, impiego di denaro, beni o utilità di provenienza illecita;
- 90igrant di 90igrant;
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, favoreggiamento personale.

Occorre tuttavia precisare che quasi tutte le fattispecie transnazionali astrattamente rilevanti per la Società – in particolare i reati associativi e quelli di riciclaggio, ma anche il delitto di induzione a rendere dichiarazione mendaci – sono già previste quali autonomi reati presupposto della

responsabilità degli enti (cioè, anche se commesse in una dimensione meramente nazionale). In questi casi, il carattere "transnazionale" non assume una funzione estensiva della responsabilità della persona giuridica ai sensi del Decreto, incidendo esclusivamente sulla comminatoria edittale di pena per il fatto commesso.

L'unica eccezione è quella del favoreggiamento personale (art. 378 c.p.), che consiste nel prestare aiuto a taluno – dopo l'avvenuta commissione di un delitto per il quale la legge stabilisce l'ergastolo o la reclusione e fuori dei casi di concorso nel medesimo – ad eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa. Il reato sussiste anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto. Si precisa che, per giurisprudenza maggioritaria, integrano il reato anche le false risposte, tese ai fini di cui sopra, alle richieste dell'autorità giudiziaria. Tali condotte assumono rilevanza, ai fini del Decreto 231, solo quando connotate dal carattere transnazionale.

7.4.2. ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Con riguardo ai delitti di criminalità organizzata, nonché a quelli con finalità di terrorismo o di eversione dell'ordine democratico e ai reati transnazionali, le possibili modalità di realizzazione delle condotte criminose sono molto ampie, in ragione del fatto che, attraverso tali fattispecie, assumono potenzialmente rilevanza (quali reati-presupposto) tutte le tipologie delittuose astrattamente configurate nell'ordinamento. La prassi giurisprudenziale, d'altra parte, ha dimostrato come, attraverso l'imputazione della fattispecie associativa o di quella transnazionale, alle persone giuridiche siano ascrivibili una serie di fattispecie autonomamente non annoverate nel catalogo dei reati-presupposto: illeciti penali tributari (ex D.lgs. n. 74/2000), reati contro il patrimonio (es. truffa ex art. 640 c.p.), reati ambientali non ricompresi nel catalogo, delitti dei privati contro la Pubblica Amministrazione (es. turbativa d'asta ex art. 353 c.p.).

In particolare, alla luce dell'attività concretamente svolta, alla Società potrebbero essere potenzialmente imputate operazioni finanziarie che integrano illeciti penali tributari, condotte di truffa ai danni degli investitori e condotte di favoreggiamento personale (transnazionale).

Ciò avverrebbe, ad esempio, qualora la SGR fosse coinvolta nella realizzazione di frodi fiscali compiute attraverso la compartecipazione di altri soggetti giuridici (persone fisiche o giuridiche), che ad esempio simulino operazioni finanziarie inesistenti e contabilizzino i relativi flussi di denaro (in entrata o in uscita), in modo da incidere sugli obblighi tributari della Società. Ancora, la SGR potrebbe essere

responsabile – di concorso, nella forma eventuale ("concorso esterno") – tutte le volte in cui presti assistenza finanziaria o comunque garantisca l'appoggio economico od operativo a persone che fanno parte di associazioni criminali o che comunque perseguono finalità di terrorismo o eversive dell'ordine democratico. Ancora, il reato di favoreggiamento personale transnazionale potrebbe concretizzarsi nel consapevole sostegno economico e finanziario a soggetti che, ad esempio, abbiano già consumato delitti di riciclaggio o reati tributari.

Alla luce di tali premesse, emerge come il rischio che siano posti in essere, nell'ambito dell'attività della Società, reati con finalità di terrorismo o di eversione dell'ordine democratico, reati di criminalità organizzata e reati transnazionali, riguarda principalmente le attività di instaurazione di rapporti con la clientela nell'ambito dei servizi prestati, nonché nei rapporti con fornitori di servizi.

Con riguardo alle fattispecie delittuose sopra individuate, i soggetti\le Unità organizzative principalmente coinvolte sono:

- Amministratore Delegato;
- Direttore Finanza e Controllo;
- Funzione Antiriciclaggio;
- Unità Analisi di Gestione;
- Unità Finanza;
- Unità Progetti Speciali.

7.4.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Tutte le attività "sensibili" nella prospettiva degli artt. 24-ter e 25-quater del Decreto devono essere svolte conformandosi alle leggi vigenti, alle norme del Codice Etico e Regolamento sulle operazioni personali, ai principi generali di comportamento enucleati nel Modello. In particolare vige il divieto di favorire, attraverso le attività tipiche svolte dalla Società, forme di associazione per delinquere o di tipo mafioso nonché terroristiche o di eversione dell'ordine democratico, anche a livello transnazionale, all'interno della Società o con la clientela.

Il rischio che siano posti in essere, nell'ambito dell'attività finanziaria, reati di criminalità organizzata, con finalità di terrorismo o di eversione dell'ordine democratico, nonché reati transnazionali (soprattutto in relazione al delitto di favoreggiamento personale), riguarda principalmente le attività di instaurazione dei rapporti con la clientela nell'ambito delle attività prestate dalla Società. Tali attività, ai fini della prevenzione dei reati in questione, si devono basare sul fondamentale principio

dell'adeguata conoscenza della clientela. Tale principio rappresenta uno dei fondamentali requisiti stabiliti dalla normativa concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Le attività "sensibili" sopra individuate, peraltro, coincidono con quelle in cui è più alto il rischio che si verifichino anche reati di riciclaggio. Pertanto, ai fini della prevenzione dei reati sopra illustrati, sono ritenuti idonei i principi di controllo e di comportamento individuati nel protocollo inerente al contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose, che impone adeguati e puntuali obblighi di identificazione e conoscenza della clientela.

7.5. DELITTI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

7.5.1 FATTISPECIE DELITTUOSA

Il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.), previsto dall'art. 25-decies del Decreto, è commesso da chi, con violenza o minaccia o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci coloro che siano chiamati a rendere dichiarazioni davanti all'autorità giudiziaria, utilizzabili in un procedimento penale, ed abbiano la facoltà di non rispondere. Tale fattispecie, qualora commessa con le caratteristiche della transnazionalità, integra anche gli estremi del reato transnazionale ai sensi della legge n. 146/2006.

La norma penale in esame tutela l'interesse al corretto svolgimento dell'attività giudiziaria e mira a prevenire comportamenti in grado di influire negativamente nell'accertamento della verità nel processo penale.

La condotta si realizza nei confronti della persona che, chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un processo penale, possa avvalersi della facoltà di non rispondere e consiste nell'indurla a non rendere le predette dichiarazioni o a rendere dichiarazioni mendaci con violenza, minaccia o con offerta o promessa di denaro o altra utilità.

Affinché si configuri l'ipotesi di responsabilità ex Decreto 231/01 è ovviamente necessario che il reato sia posto in essere nell'interesse o a vantaggio della Società.

7.5.2 ATTIVITÀ SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Nell'operatività della Società, il reato di cui all'art. 377-bis c.p. è astrattamente realizzabile nella gestione dei contenziosi giudiziali e stragiudiziali (es. civili, tributari, giuslavoristici, amministrativi, penali, etc.), nella nomina dei legali e nel coordinamento delle loro attività, nei rapporti con tutti i soggetti – interni o esterni – che siano chiamati a rendere dichiarazioni (ad esempio di tipo testimoniale o peritale) ad una autorità giudiziaria.

A titolo esemplificativo e non esaustivo, rientra nel caso in esame l'ipotesi in cui un dipendente della Società, imputato in un procedimento penale, chiamato a rendere dichiarazioni in un procedimento connesso in cui l'amministratore è imputato del reato di false comunicazioni sociali, riceva un'offerta di denaro per rendere dichiarazioni non corrispondenti al vero, ovvero a tal fine venga minacciato o

aggredito. Parimenti, il reato si realizza qualora si ponga in essere, ad esempio, una condotta istigatrice di un consulente tecnico o di un perito chiamato a deporre nel corso di un procedimento giudiziario.

Con riguardo alle fattispecie delittuose sopra individuate, i soggetti\le Unità organizzative principalmente coinvolte sono:

- Presidente del Consiglio di Amministrazione;
- Amministratore Delegato;
- Direttore Finanza e Controllo;
- Unità Affari Legali e Societari;
- Unità Analisi di Gestione;
- Unità Finanza.

7.5.3 PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Tutte le attività "sensibili" nella prospettiva dell'art. 377-bis c.p. devono essere svolte conformandosi alle leggi vigenti, alle norme del Codice Etico e del Regolamento sulle operazioni personali, ai principi generali di comportamento enucleati nel Modello.

La Società è conscia della delicatezza e dell'importanza che assume l'attività di amministrazione della giustizia e l'attività giudiziaria in particolare.

Pertanto, tutti i rapporti con i soggetti, pubblici o privati, che a vario titolo partecipino o siano coinvolti in procedimenti giudiziari in cui sia parte la Società (magistrati, Polizia Giudiziaria, ufficiali giudiziari, altri pubblici ufficiali, incaricati di pubblico servizio o esercenti servizi di pubblica necessità, persone offese, indagati, imputati, attori e convenuti, consulenti, periti, persone informate dei fatti testimoni) devono essere ispirati al rigoroso rispetto della normativa di legge e regolamentare vigente, nonché gestiti con la massima trasparenza, chiarezza, correttezza.

Per tale motivo, la Società, quando non vi sia obbligo di compimento di atti da parte di soggetti diversi, riserva tali rapporti all'Unità Affari Legali e Societari, che conserverà la documentazione e terrà traccia dei rapporti medesimi, comunicando sempre in via formale e per iscritto. Quando i procedimenti giudiziari coinvolgono, o possono coinvolgere, dipendenti, agenti, ex dipendenti o ex agenti, l'Unità Affari Legali e Societari collabora con l'Unità Finanza.

La Società, ogniqualvolta lo ritenga necessario, ovvero per le attività di assistenza e rappresentanza in giudizio, sentito il parere dell'Unità Affari Legali e Societari, conferisce formale incarico a professionisti

iscritti all'Ordine degli Avvocati, unicamente ai quali è demandato il contatto con i soggetti di cui sopra, ivi compresa l'eventuale attività investigativa ai sensi degli articoli 391 bis e segg. C.p.p., nel rispetto delle norme di legge e del codice deontologico professionale.

I destinatari del Modello che dovessero essere coinvolti a vario titolo in procedimenti giudiziari in cui siano coinvolte la SGR o altre società del Gruppo, o nei quali le stesse dovessero avere un interesse anche indiretto, ovvero per ragioni connesse all'attività delle società medesime, devono senza indugio darne comunicazione al proprio superiore gerarchico e all'Unità Affari Legali e Societari, salvo il caso in cui gli stessi rivestano, anche di fatto, la qualità di "controparte" delle società.

Infine, al fine di fornire all'Organismo di Vigilanza gli strumenti per esercitare le sue attività di monitoraggio e di verifica puntuale dell'efficace esecuzione dei controlli previsti dal Modello, a prescindere dagli altri obblighi di segnalazione, tutti i soggetti interessati sono tenuti a comunicare all'Organismo di Vigilanza il manifestarsi del singolo evento (i.e. notifica di una citazione in qualità di testimone) cui sono legati i rischio-reato e i controlli attesi.

7.6. FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

L'art. 25-bis del Decreto 231/01, aggiunto dal D.L. 25 settembre 2001, n. 350, riguarda i delitti previsti dal codice penale in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

Si osserva che la Società non detiene somme di denaro per conto dei clienti: queste ultime sono infatti depositate in un conto appositamente aperto dalla SGR presso la banca depositaria, con l'indicazione che si tratta di un conto corrente c/terzi, e che quindi le fattispecie di delitti previsti dall'art. 25-bis del Decreto non sono di immediato interesse per la stessa.

7.6.1 FATTISPECIE DELITTUOSE

Si elencano di seguito le fattispecie contemplate dall'art. 25-bis del Decreto:

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- alterazione di monete (Art. 454 c.p.);
- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- uso di valori di bollo contraffatti o alterati (art. 464 c.p.).

Si ritiene invece astrattamente configurabile un rischio – seppur alquanto remoto – per la Società in ordine alla fattispecie del reato di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.), che si configura nel caso in cui chiunque, potendo conoscere l'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati. Fattispecie parzialmente connessa,

anch'essa rientrante nell'illecito amministrativo di cui all'art. 25-bis D.Lgs 231/01, è poi quella di cui all'art. 474 c.p. che sanziona l'introduzione nello Stato e il commercio di prodotti con segni falsi.

7.6.2 ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Le attività aziendali "sensibili" identificate dal Modello, nelle quali è maggiore il rischio che siano posti in essere i reati sopra illustrati, sono la gestione della liquidità e dei valori di bollo.

Ancorché improbabile, quanto invece alla falsità in strumenti e segni di riconoscimento, si ritiene che l'unica attività "sensibile" sia quella di creazione da parte della Società di nuovi marchi o segni distintivi da utilizzare per le proprie attività, iniziative o prodotti: in tale caso, la Società potrebbe utilizzare, anche inavvertitamente, marchi già soggetti a registrazione.

7.6.3 PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Nonostante la possibilità di commissione da parte dei destinatari del Modello nell'interesse o vantaggio della SGR dei reati previsti dal Decreto in materia di falsità in monete, carte di pubblico credito e valori di bollo presenti un basso profilo di rischiosità, la Società intende assumere un ruolo attivo nella tutela di quella particolare forma della fede pubblica che si concretizza nell'esigenza di certezza ed affidabilità del traffico economico-giuridico, con specifico riferimento all'affidamento del pubblico sulla genuinità del mezzo di scambio rappresentato dalla moneta e sulla genuinità dei valori di bollo distribuiti o ricevuti dalla SGR, anche al fine di prevenire i residui rischi ipotizzabili in ordine alla commissione dei reati di cui all'art. 25-bis del Decreto da parte dei propri esponenti aziendali.

Le attività "sensibili" sopra individuate coincidono con quelle in cui è più alto il rischio che si verifichino anche reati societari. Pertanto, ai fini della prevenzione dei reati sopra illustrati, sono ritenuti idonei i principi di controllo e di comportamento individuati nel protocollo inerente i reati societari, con particolare riguardo alla gestione della liquidità aziendale.

7.7. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, AUTORICICLAGGIO

L'art. 25 octies del D.Lgs. 231/2001, introdotto dal D.Lgs. n. 231/2007 (anche "Decreto antiriciclaggio", nel seguito), ha esteso la responsabilità dell'Ente ai reati di ricettazione, riciclaggio, impiego illecito di denaro, beni o utilità, a prescindere dal fatto che siano commessi con finalità di terrorismo o di eversione dell'ordine democratico (in ordine alle quali si rimanda all'apposito paragrafo) e autoriciclaggio (introdotto con la L. 186/14). La finalità del rafforzamento della disciplina della responsabilità amministrativa degli Enti consiste nel prevenire e reprimere più efficacemente il fenomeno dell'immissione nel circuito economico lecito di denaro, beni od utilità provenienti dalla commissione di delitti, in quanto di ostacolo all'amministrazione della giustizia nelle attività di accertamento dei reati e di persecuzione dei colpevoli, oltre che, più in generale, lesiva dell'ordine economico, dell'integrità dei mercati e della libera concorrenza, in ragione degli indebiti vantaggi competitivi di cui godono gli operatori che dispongono di capitali di origine illecita.

Su un piano diverso, ma pur sempre finalizzate al contrasto del riciclaggio e del finanziamento del terrorismo, si collocano le previsioni contenute nel Decreto antiriciclaggio, e successive modifiche ed integrazioni, di specifici adempimenti posti a carico delle banche e degli intermediari finanziari in genere (adeguata verifica della clientela; conservazione della documentazione; segnalazione di operazioni sospette; comunicazioni delle violazioni dei divieti in tema di denaro contante e dei titoli al portatore; comunicazione da parte degli Organi di controllo dell'Ente delle infrazioni riscontrate; formazione del personale). La violazione di detti obblighi è di per sé sanzionata, ma non comporta la responsabilità amministrativa dell'Ente ai sensi del D.Lgs. 231/2001, non essendo detti illeciti ricompresi nell'elencazione dei cosiddetti reati presupposto. Ciò non toglie che i presidi adottati dalla Società nell'ambito della normativa di settore di cui al citato D.Lgs 231/07 rappresentano fondamentali strumenti di prevenzione, organizzazione e controllo nella mitigazione dei rischi reato di cui agli artt. 648 c.p. e ss. Per questa ragione, i protocolli 231 adottati dalla Società in relazione ai reati di riciclaggio sono profondamente connessi e agganciati alle procedure aziendali in materia AML.

Il Decreto antiriciclaggio, e le successive modifiche e integrazioni, con la previsione di sanzioni per le infrazioni di tali obblighi, ha inteso istituire una tutela preventiva, che prescinde dal ricorrere nelle concrete fattispecie di ipotesi di riciclaggio, ma che mira comunque ad assicurare il rispetto dei fondamentali principi della approfondita conoscenza della clientela e della tracciabilità delle transazioni, al fine di scongiurare anche il mero pericolo di inconsapevole coinvolgimento degli

intermediari finanziari in fatti di ricettazione, riciclaggio e impiego illecito di capitali. È importante sottolineare che qualora l'operatore della SGR contravvenisse a detti adempimenti nella consapevolezza della provenienza illecita dei beni oggetto delle operazioni, potrebbe essere chiamato a rispondere per i predetti reati, e potrebbe quindi conseguirne anche la responsabilità amministrativa della SGR ai sensi del D.Lgs. 231/2001.

7.7.1. FATTISPECIE DELITTUOSE

Reati presupposto dell'illecito amministrativo di cui all'art. 25-octies D.Lgs. 231/01 emersi come potenzialmente rilevanti per la Società all'esito del Risk Assessment:

Ricettazione (art. 648 c.p.)

Commette il reato di ricettazione chiunque, allo scopo di procurare a sè o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare. Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni di provenienza delittuosa. E' inoltre richiesta la conoscenza della provenienza delittuosa del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi ed univoche – quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni – da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della provenienza illecita del denaro o del bene.

Riciclaggio (art. 648-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni od altre utilità provenienti da un delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. La norma va interpretata come volta a punire coloro che – consapevoli della provenienza delittuosa di denaro, beni o altre utilità – compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati. Non è richiesto, ai fini del perfezionamento del reato, l'aver agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento.

Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione. Con riferimento ai rapporti bancari, ad esempio, la semplice accettazione di un deposito potrebbe integrare la condotta di sostituzione tipica del riciclaggio (sostituzione del denaro contante con moneta scritturale, quale è il saldo di un rapporto di deposito). Come per il reato di ricettazione, la consapevolezza dell'agente in ordine alla provenienza illecita può essere desunta da qualsiasi circostanza oggettiva grave ed univoca.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

La condotta criminosa si realizza attraverso l'impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio) c.p. Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648 ter circoscrive la condotta all'impiego di tali risorse in attività economiche o finanziarie.

Autoriciclaggio (art. 648-ter. 1 c.p.)

La condotta criminosa si realizza attraverso l'impiego, la sostituzione, il trasferimento in attività economiche, finanziarie, imprenditoriali o speculative, di denaro, beni o le altre utilità provenienti da un delitto non colposo che – differentmente dalle fattispecie sopra descritte – si è commesso o è concorso a commettere, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Se i proventi derivano dalla commissione di un delitto doloso per il quale è stabilita la pena della reclusione nel massimo fino a cinque anni, si applica la pena della reclusione da uno a quattro anni. La pena è aumentata se il fatto è commesso nell'esercizio di un'attività professionale, bancaria o finanziaria. La pena è diminuita per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. Inoltre, non sono punibili le condotte per cui il denaro, i beni e le altre utilità vengono destinate alla mera utilizzazione o godimento personale.

Va peraltro aggiunto che il reato di autoriclaggio rileva, in prospettiva 231, sotto un duplice profilo, in termini parzialmente simili a ciò che avviene per i reati associativi. Da una parte, come si è detto, rappresenta un rischio-reato diretto per l'Ente (ossia l'attività dell'ente risulta esposta direttamente alla commissione, da parte di un suo esponente, del reato di autoriciclaggio); dall'altra, l'Ente

potrebbe risultare esposto indirettamente ai rischi reato conessi al delitto presupposto del reato di autoriciclaggio. Ci si riferisce, in particolare, alla possibilità che l'Ente (sulla base di una interpretazione estensiva molto severa) venga chiamato a rispondere, secondo i criteri di imputazione ex D.Lgs 231/01, per l'inidoneità dei suoi presidi in relazione non tanto e non solo al rischio diretto di autoriciclaggio, quanto in relazione ai singoli delitti che hanno generato la provvista poi autoriclata dall'Ente. In questa prospettiva, considerando quanto emerso dal Risk Assessment, potrebbero venire in rilievo, ad esempio e principalmente, alcune fattispecie di reato tributario non comprese nel catalogo dei "reati presupposto 231" quali le ipotesi di cui agli art. 4, 5 e 10-quater D.lgs 74/2000 (nella loro tipicità "classica" e non già rientrante nel comma 1-bis dell'art. 25-quinquiesdecies D.Lgs 231/01) e in relazione ai quali l'Ente ha comunque adottato specici protocolli 231 elencati nella Parte Speciale dedicata ai reati tributari, a cui si rinvia.

7.7.2. ATTIVITÀ AZIENDALI SENSIBILI

Le attività aziendali sensibili identificate dal Modello, nelle quali è maggiore il rischio che siano posti in essere i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, sono le seguenti:

- gestione di rapporti diretti con clientela o fornitori e di eventuali adempimenti antiriciclaggio nei confronti della clientela (quali identificazione delle controparti contrattuali e/o registrazione delle relative operazioni);
- gestione della liquidità e di valori di bollo;
- gestione della tesoreria e delle risorse finanziarie;
- gestione della contabilità e del bilancio;
- gestione degli adempimenti fiscali connessi alla Società, al gruppo e agli OICR.

In particolare, possono individuarsi le seguenti modalità di realizzazione della condotta:

- acquisto, ricezione od occultamento di denaro o cose provenienti da un qualsiasi delitto, ovvero compimento, in relazione ad essi, di atti volti a farli acquistare, ricevere od occultare;
- sostituzione o trasferimento di denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compimento in relazione ad essi di altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa;
- impiego in attività economiche o finanziarie (salvo che in ipotesi di concorso nel reato, ricettazione o riciclaggio), di denaro, beni o altre utilità provenienti da delitto;

- impiego in attività economiche o finanziarie, o con finalità speculative, di proventi derivanti da delitto non colposo, con la finalità di ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Per quanto attiene agli obblighi antiriciclaggio che la Società è tenuta a rispettare, la violazione degli stessi può avere una rilevanza anche ai fini del Decreto 231/01 soltanto in caso di mancata segnalazione di operazioni sospette caratterizzata dalla volontà di coprire l'operazione di riciclaggio o di finanziamento al terrorismo del cliente, in quanto in tale ipotesi la Società concorrerebbe nella commissione del reato da parte del cliente. In tale contesto, rileva la corretta gestione del processo interno che porta alla decisione di effettuare, oppure no, una segnalazione di operazione sospetta; in particolare, con riguardo ai casi in cui la Società decida di non effettuare una segnalazione, la formalizzazione delle analisi condotte e delle ragioni alla base di tale decisione da parte delle competenti funzioni aziendali ed una verifica del rispetto dell'obbligo di formalizzazione e dei relativi contenuti sono fondamentali a presidio del concorso della Società nella commissione dei reati di riciclaggio e finanziamento al terrorismo.

Con riguardo alle fattispecie delittuose sopra individuate, le Unità organizzative principalmente coinvolte sono:

- Consiglio di Amministrazione;
- Amministratore Delegato;
- Direttore Finanza e Controllo;
- Funzione Antiriciclaggio;
- Unità Finanza;
- Direttore Commerciale;
- Unità Analisi di Gestione.

7.7.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Si riportano di seguito i principi di controllo e di comportamento applicabili all'instaurazione e alla gestione dei rapporti continuativi con la clientela nonché al trasferimento di fondi, che si completano con le procedure aziendali di dettaglio che regolamentano le medesime attività.

Ai fini del contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose, si rimanda ai seguenti ambiti di operatività:

- identificazione e conoscenza della clientela e dei soggetti per conto dei quali i clienti operano, valutandone il profilo di rischio;
- apertura di nuovi rapporti continuativi e aggiornamento/revisione delle informazioni sui clienti esistenti;
- monitoraggio dell'operatività della clientela secondo tempistiche e modalità stabilite con riferimento al profilo di rischio assegnato, ed in particolare valutazione dell'operatività disposta dalla clientela riguardante soggetti/Paesi/merci/settori oggetto di restrizioni di natura finanziaria e/o commerciale;
- assolvimento degli obblighi normativi in materia di conservazione delle informazioni relative ai rapporti continuativi e alle operazioni disposte dalla clientela;
- reporting esterno indirizzato alle Autorità di Vigilanza.

Il sistema di controllo a presidio dei processi descritti si basa sui seguenti principi:

- responsabilità definite: le procedure interne, qui integralmente richiamate, individuano i soggetti e le strutture responsabili dell'attivazione/gestione dei processi sopra descritti e dei relativi controlli;
- segregazione dei compiti:
  - nelle situazioni che impongono obblighi rafforzati di adeguata verifica della clientela, subordinazione – al rilascio di una autorizzazione da parte del Responsabile Aziendale Antiriciclaggio e/o dell'Amministratore Delegato – dell'apertura di nuovi rapporti, del mantenimento di rapporti preesistenti e dell'esecuzione delle operazioni;
  - in relazione alle attività di monitoraggio dell'operatività, volte ad individuare operazioni potenzialmente sospette, esistenza di una segregazione in base alla quale:
    - le funzioni aziendali competenti monitorano le operazioni relative alla propria area, segnalando i movimenti anomali al Responsabile Aziendale Antiriciclaggio per gli opportuni approfondimenti e/o segnalazioni;
    - il Responsabile Aziendale Antiriciclaggio effettua l'analisi della segnalazione e svolge le necessarie indagini sull'operazione sospetta, disponendo l'inoltro o meno – dopo un confronto con l'Amministratore Delegato – delle segnalazioni alla competente Autorità;
- attività di controllo:

- verifica, nell'ambito di una puntuale profilatura della clientela, all'atto dell'accensione del rapporto da parte della Direzione Commerciale, della correttezza e completezza dei dati e delle informazioni fornite dalla clientela;
- verifica da parte della Direzione Commerciale dell'eventuale presenza del nominativo nelle versioni aggiornate delle liste antiterrorismo;
- controllo incrociato, da parte della Direzione Commerciale, tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento, i fondi impiegati, l'orizzonte temporale dell'investimento, il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
- monitoraggio e presidio, da parte delle funzioni di controllo, della puntuale esecuzione delle attività delle unità operative in merito alla:
  - acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
  - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;
  - conservazione dei documenti e delle informazioni;
- controllo autonomo, da parte del Responsabile Aziendale Antiriciclaggio, sull'operatività di tutti i clienti rientranti nei "pattern" di controllo definiti dal Consiglio di Amministrazione;
- controllo autonomo, da parte del Responsabile Aziendale Antiriciclaggio, nell'ambito delle dinamiche infragruppo e nel rapporto con piattaforme di distribuzione, consistente in verfiche campionarie svolte presso il Transfer Agent di Kairos International Sicav;
- tutti i documenti, i dati e le informazioni devono essere conservati con modalità che ne assicurino l'accessibilità completa e tempestiva da parte delle Autorità, la tempestiva acquisizione da parte del soggetto obbligato, l'integrità, la non alterabilità, la trasparenza, la completezza, la chiarezza, nonché il mantenimento della storicità;

- tracciabilità del processo sia a livello di sistema informativo sia in termini documentali;
- riservatezza delle informazioni, con particolare riguardo a quelle relative ai titolari effettivi e ai fiduciani, nonché ai processi di monitoraggio delle operazioni e di segnalazione delle operazioni sospette;
- formazione.

Con specifico riferimento ai reati di riciclaggio e omessa segnalazione di operazioni sospette, l'iter procedurale previsto all'interno della SGR è basato sui seguenti presidi:

- riciclaggio:
    - previsione di appositi poteri di spesa, già richiamati nell'ambito dei reati societari, che prevedono, per importi rilevanti, la doppia firma;
    - previsione di limitazioni dei poteri di spesa sulla base della posizione apicale ricoperta dal soggetto;
- segnalazione di operazioni sospette:
    - previsione di apposito report, sottoscritto dal Responsabile Aziendale Antiriciclaggio e dall'Amministratore Delegato, a conclusione dell'analisi svolta sulle operazioni potenzialmente sospette, sia in caso di inoltro all'UIF, sia in caso di non necessario invio.

Con specifico riferimento alla gestione della tesoreria e delle risorse finanziarie, alla gestione della contabilità e del bilancio, nonché alla gestione degli adempimenti fiscali connessi alla Società, al gruppo e agli OICR, i presidi adottati sono dettagliatamente descritti rispettivamente nelle procedure:

- "Contabilità e bilancio – Gestione dell'attivo patrimoniale";
- "Contabilità e bilancio – Gestione dell'attivo patrimoniale", "Criteri di valutazione degli strumenti finanziari", "Processo di valorizzazione", "Prezzi di trasferimento per transazioni infragruppo", "Linee guida per la revisione";
- "Adempimenti fiscali", "Codice di condotta in materia fiscale", "FATCA e QI", "CRS", "Manuale QI" e "Prezzi di trasferimento per transazioni infragruppo".

7.8. REATI ED ILLECITI AMMINISTRATIVI RICONDUCIBILI AD ABUSI DI MERCATO

L'art. 25-sexies del Decreto include tra i reati presupposto della responsabilità ai sensi del Decreto anche le fattispecie di reato relative ai c.d. abusi di mercato, ossia i reati di abuso di informazioni privilegiate e di manipolazione del mercato previste ai sensi degli artt. 184 e 185 del T.U.F.

L'ambito della condotta vietata è delineato dagli articoli del T.U.F. richiamati in conformità con le previsioni del Regolamento (UE) n. 596/2014 ("MAR") e della Direttiva 2014/57/UE (c.d. "MAD II").

In particolare, la MAR ha introdotto un quadro normativo uniforme nell'Unione Europea in materia di abusi di mercato, in sostituzione della disciplina precedentemente prevista da ciascun ordinamento degli Stati Membri in attuazione della abrogata direttiva 2003/6/CE.

Oltre alle fattispecie di reato richiamate espressamente dall'art. 25-sexies del Decreto, il T.U.F. prevede delle fattispecie di illecito amministrativo ai sensi degli artt. 187-bis e 187-ter del T.U.F., rispettivamente per il caso di abuso e comunicazione illecita di informazioni privilegiate in violazione dell'art. 14 MAR nonché per il caso di manipolazione del mercato ai sensi dell'art. 15 MAR.

Lo stesso T.U.F. (art. 187-quinquies), poi, prevede una potenziale responsabilità amministrativa per gli enti, in aggiunta a quella prevista dal Decreto, per il caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui all'articolo 14 MAR o del divieto di cui all'articolo 15 del MAR, con regole di imputabilità per l'Ente analoghe a quelle del D. Lgs. N. 231/2001.

L'187 ter.1 del T.U.F., inoltre, introdotto dal D. lgs. 10 agosto 2018, n. 107, prevede sanzioni amministrative a carico di ciascun ente o società per la violazione di disposizioni specifiche contenute nel MAR.

Le predette norme mirano a garantire l'integrità, la trasparenza, la correttezza e l'efficienza dei mercati finanziari in ottemperanza al principio per cui tutti gli investitori debbono operare in condizioni di uguaglianza sotto il profilo dell'accesso all'informazione, della conoscenza del meccanismo di fissazione del prezzo e della conoscenza delle origini delle informazioni pubbliche.

Salvo quanto meglio si specificherà con riferimento a ciascuno dei diversi illeciti, le condotte di abuso di mercato possono avere per oggetto:

- strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altri Stati membri dell'Unione europea;
- strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata richiesta di ammissione alle negoziazioni in un sistema multilaterale di negoziazione (c.d. MTF) italiano o di altri Stati membri dell'Unione europea;
- strumenti finanziari negoziati su un sistema organizzato di negoziazione (c.d. OTF) italiano o di altri Stati membri dell'Unione europea;
- altri strumenti finanziari non contemplati nei punti precedenti, il cui prezzo dipende da prezzi di strumenti negoziati nelle sedi di cui ai precedenti punti o ha effetto sugli stessi, compresi i credit default swap e i contratti differenziali.

Le condotte di abuso di mercato possono anche avere ad oggetto anche alle condotte o alle operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010.

Va precisato che ai sensi dell'art. 182 del T.U.F. le condotte sanzionate sono punite secondo la legge italiana, anche se commesse all'estero, qualora attengano a strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o in un sistema multilaterale di negoziazione italiano per i quali l'ammissione è stata richiesta o autorizzata dall'emittente, oppure attengano a strumenti finanziari negoziati su un sistema organizzato di negoziazione italiano. Nel caso in cui i fatti siano commessi in Italia, le medesime condotte sono sanzionate se riferite a strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altri Paesi dell'Unione europea.

Si rammenta altresì che tra i reati che possono dar luogo alla responsabilità degli Enti vi è anche il reato di aggiotaggio (art. 2637 c.c.) che, ancorché incluso nei "reati presupposto" societari di cui all'art. 25-ter del Decreto, è riconducibile, al tempo stesso, alla materia degli abusi di mercato in senso lato, ancorchè le fattispecie di reato fanno riferimento a "strumenti finanziari non quotati, o per i quali non é stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato".

I maggiori rischi in relazione alla commissione degli illeciti della specie si possono ipotizzare nei seguenti casi:

- operazioni simulate, altri artifici o abuso di informazioni privilegiate per conto della SGR o a favore di clienti della stessa, ove sussista un interesse o vantaggio della SGR medesima;
- diffusione di notizie false o fuorvianti, soprattutto in correlazione ad operazioni effettuate sul mercato, prima o dopo tale diffusione.

In presenza di operazioni richieste dai clienti che facciano sospettare la commissione di uno degli illeciti di "Abuso di informazione privilegiata" o di "Manipolazione del mercato", esiste un obbligo di segnalazione in capo all'intermediario; tuttavia non può escludersi che, in astratto, si possa configurare un coinvolgimento della SGR nell'illecito commesso dal cliente in relazione alle concrete modalità di svolgimento delle attività da parte della SGR.

7.8.1. FATTISPECIE DELITTUOSE

Si fornisce di seguito una descrizione delle fattispecie di reato.

Abuso di informazioni privilegiate (art. 184 T.U.F.)

La fattispecie penale si realizza quando un soggetto in possesso di informazioni privilegiate in ragione (i) della sua qualità di membro degli organi di amministrazione, direzione o controllo dell'emittente ovvero (ii) della partecipazione al capitale dell'emittente ovvero (iii) dell'esercizio di un'attività lavorativa, professionale ovvero di una funzione, anche pubblica, o di un ufficio:

(a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime (insider trading);
(b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'art. 11 MAR (comunicazione illecita di informazioni privilegiate o tipping);
(c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a) (raccomandazioni o tuyautage).

Il reato di abuso di informazioni privilegiate di cui all'art. 184 del T.U.F. può, inoltre, essere commesso da chi sia entrato in possesso di informazioni privilegiate in conseguenza della preparazione o

commissione di un reato (es. intrusione in un sistema informatico ed estrazione di informazioni privilegiate). La fattispecie si realizza altresì quando detti soggetti comunicano dette informazioni privilegiate al di fuori dell'esercizio del proprio lavoro o professione ed anche quando raccomandano o inducono altri soggetti, sulla scorta delle informazioni privilegiate di cui sono in possesso, a compiere talune delle operazioni sopradescritte.

Per informazione privilegiata, ai sensi dell'art. 7 MAR (come anche richiamato dall'art. 180, comma 1, lett. B-ter, del T.U.F.) si intende "un'informazione avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari, e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati".

Un'informazione si ritiene di carattere preciso se:

- fa riferimento a una serie di circostanze o a un evento verificatisi o che si può ragionevolmente ritenere che vengano a prodursi e
- se tale informazione è sufficientemente specifica da permettere di trarre conclusioni sul possibile effetto sui prezzi degli strumenti finanziari o del relativo strumento finanziario derivato, dei contratti a pronti su merci collegati o dei prodotti oggetto d'asta sulla base delle quote di emissioni.

Per informazione che, se comunicata al pubblico, avrebbe probabilmente un effetto significativo sui prezzi s'intende un'informazione che un investitore ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento.

Nel caso delle persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari

Nell'ambito dell'operatività della SGR, si riscontrano numerose fattispecie nelle quali possono profilarsi elementi di rischio, che possono comportare la responsabilità della SGR nel caso in cui il reato sia commesso nell'interesse, esclusivo o concorrente, dell'Ente stesso.

Manipolazione del mercato (art. 185 T.U.F.)

La fattispecie penale si realizza quando qualcuno diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

Non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'art. 13 del MAR.

Le disposizioni contenute nell'art. 185 TUF si applicano anche:

- ai fatti concernenti i contratti a pronti su merci che non sono prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari;
- ai fatti concernenti gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari;
- ai fatti concernenti gli indici di riferimento (i c.d. benchmark), come definiti nell'articolo 3, paragrafo 1, punto 29), del MAR.

Aggiotaggio (art. 2637 c.c.)

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Sanzioni amministrative: abuso e comunicazione illecita di informazioni privilegiate e manipolazione del mercato (art. 187-bis e art. 187-ter T.U.F.)

Gli illeciti amministrativi di cui agli artt. 187 bis e 187 ter del TUF prevedono fattispecie sostanzialmente speculari a quelle contemplate come figure di reato dagli artt. 184 e 185, disponendo l'applicazione di sanzioni amministrative in capo alla persona fisica (oltre che all'ente, nel caso in cui la violazione sia commessa nel suo interesse o a suo vantaggio) che violi il divieto di abuso di

informazioni privilegiate e di comunicazione illecita di informazioni privilegiate e il divieto di manipolazione del mercato di cui agli articoli 14 e 15 del MAR.

Il rinvio diretto a tali articoli comprende tutti gli elementi a loro volta implicitamente richiamati dalle due fattispecie disciplinate dal MAR. Ciò implica che la condotta rilevante ai fini dell'applicazione della sanzione amministrativa risulta più ampia di quella rilevante ai fini penali, quest'ultima circoscritta agli elementi espressamente descritti dal T.U.F. per i quali non opera un generale rinvio al MAR (a titolo d'esempio, la condotta chi ha ricevuto le informazioni privilegiate dai c.d. insider primari non è punibile penalmente ai sensi dell'art. 184 del T.U.F., mentre rileva ai fini dell'applicazione dell'art. 187-bis, in forza del richiamo dell'art. 14 del MAR; la condotta che integra l'illecito amministrativo di manipolazione del mercato ha una estensione più ampia rispetto alla corrispondente fattispecie penale, posto che il reato prevede la diffusione di notizie false o il compimento di operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, mentre l'illecito amministrativo contempla diverse ulteriori condotte quali, ad es., la diffusione, tramite mezzi di informazione, compreso internet o ogni altro mezzo, di informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti e il compimento di operazioni idonee a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari').

Inoltre, mentre per la configurazione di un illecito penale è necessaria l'esistenza del dolo, per l'illecito amministrativo è sufficiente la colpa.

Ciò non esclude che le medesime condotte possano essere rilevanti ai fini sia penali e sia amministrativi, potendo dare origine ad un cumulo di sanzioni.

7.8.2. ATTIVITÀ AZIENDALI SENSIBILI

Le attività "sensibili" identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati e gli illeciti amministrativi riconducibili ad abusi di mercato sono le seguenti:

- gestione e divulgazione delle informazioni e delle comunicazioni esterne;
- gestione delle operazioni di mercato;
- attività ordinaria dei soggetti appartenenti alla Direzione Commerciale, all'Unità Consulenza, all'Unità Trading Desk e RTO e all'Unità Operations (Amministrazione Clienti).

7.8.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Si riportano di seguito, per ognuna delle sopraelencate attività "sensibili", i principi di controllo e di comportamento applicabili a dette attività, che si completano con la normativa aziendale di dettaglio che le regolamenta.

Con riferimento alla gestione e alla divulgazione delle informazioni e delle comunicazioni esterne, ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato, il sistema di controllo a presidio si basa sui seguenti principi:

- istituzione e gestione di una "Restricted List" in cui annotare le eventuali informazioni privilegiate ricevute nell'ambito delle attività poste in essere dai dipendenti e collaboratori e, più in generale, da tutti i soggetti che a vario titolo operano in nome e/o per conto della Società;
- definizione di apposite procedure interne che delineano il processo per l'alimentazione e la gestione della lista, nonché le funzioni aziendali tempo per tempo responsabili della gestione medesima;
- implementazione di sistemi di sicurezza logica e di altre procedure, a garanzia della corretta gestione delle informazioni;
- separatezza organizzativa tra le unità che potrebbero avere a disposizione informazioni privilegiate e le altre unità operative;
- implementazione di misure procedurali e organizzative per la prevenzione degli illeciti in tema di abusi di mercato (a titolo esemplificativo, si pensi alle richieste finalizzate alla valutazione di una informazione come "price sensitive" o privilegiata);
- monitoraggio delle attività di compravendita di strumenti finanziari poste in essere dalla SGR per conto dei patrimoni gestiti;
- divieto di utilizzo di "informazioni privilegiate" da parte di chiunque ne venga, a qualunque titolo, a conoscenza; tale divieto vige sia qualora un eventuale impiego delle stesse vada a proprio personale vantaggio; sia nel caso in cui tale utilizzo possa arrecare un vantaggio a terzi; sia nel caso in cui il loro utilizzo possa favorire o determinare un vantaggio per la Società;
- divieto di diffusione di "informazioni privilegiate" all'interno e/o all'esterno della Società, fuori dai casi in cui ciò sia strettamente necessario per il corretto e diligente adempimento delle proprie mansioni, da effettuarsi comunque nel rispetto dei previsti obblighi di legge;

- obbligo di tempestiva comunicazione dell'"informazione privilegiata"al Responsabile dell'Unità Compliance, che provvederà senza indugio alla relativa iscrizione nella "Restricted List", ai necessari accertamenti e ad attivare le azioni conseguenti;
- obbligo di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la SGR, o le altre società del Gruppo, sia riguardanti società terze oggetto di investimento da parte della SGR, nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- divieto di compiere operazioni che anticipino le operazioni della clientela e dei patrimoni gestiti sugli stessi strumenti;
- divieto di trasmettere a terzi informazioni sugli ordini o sulle informazioni ricevute dalla clientela e/o acquisite nell'ambito dello svolgimento delle funzioni di gestione;
- divieto di comunicare informazioni a terzi per ragioni diverse da quelle di ufficio, ovvero raccomandare o indurre terzi a compiere operazioni connesse alle informazioni privilegiate;
- divieto di discutere informazioni privilegiate in luoghi pubblici o in locali in cui siano presenti estranei o comunque soggetti che non hanno necessità di conoscere tali informazioni;
- divieto di diffondere, sia ad altro personale sia all'esterno della SGR, informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti;
- divieto di produrre e diffondere studi e ricerche o altre comunicazioni di marketing, acquisite nell'ambito dell'attività lavorativa, in violazione delle norme, interne ed esterne, e, in particolare, senza garantire un'informazione chiara, corretta e non fuorviante;
- obbligo di custodire accuratamente documenti contenenti informazioni confidenziali e riservate, di assicurarsi che le proprie password rimangano segrete e che il proprio computer sia adeguatamente protetto, attraverso il blocco temporaneo dello stesso nei momenti in cui ci si allontana dalla propria postazione.

Obiettivo delle regole sancite dal presente paragrafo, in ottemperanza ai dettami della normativa vigente, è quello di garantire che nella esecuzione delle operazioni di negoziazione e regolamento sul mercato – ovvero nelle modalità di inoltro degli ordini a soggetti terzi per la loro esecuzione – non siano poste in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, ovvero non siano poste in essere operazioni o altri artifizi idonei a fornire indicazioni false e fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

In relazione alle attività compiute dalla SGR per conto dei portafogli gestiti è prevista l'attivazione di procedure interne per la segnalazione delle operazioni sospette, successivamente al compimento delle stesse.

Con riferimento alla gestione delle operazioni di mercato, ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato, il sistema di controllo a presidio si basa sui seguenti principi:

- livelli autorizzativi definiti e, in particolare, approvazione da parte degli Organi competenti in base al vigente sistema dei poteri e delle deleghe:
  - dei limiti a cui devono uniformarsi i vari team di gestione nelle scelte di investimento effettuate per conto dei portafogli gestiti;
  - dei limiti operativi previsti dal "Processo di investimento" sugli strumenti presenti nelle "liste" previste dalle procedure interne ("Watch List", "Restricted List" e "Group Holdings");
- attività di controllo automatico sulle operazioni di compravendita titoli eseguite sui mercati[7];
- monitoraggio delle attività relative alla prestazione di servizi di gestione collettiva e gestione di portafogli da parte delle funzioni di controllo della SGR;
- tracciabilità del processo, sia a livello di sistema informativo sia in termini documentali;
- divieto di diffondere notizie false, di indicare alle proprie controparti, investitori o clienti, come fondate, notizie generiche e non confermate;
- divieto di utilizzare, nei colloqui con le controparti, investitori o clienti, termini o espressioni consapevolmente iperboliche, suggestive o denigratorie, allo scopo di trarre in inganno la controparte, l'investitore o il cliente;
- divieto di porre in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari;
- divieto di compiere operazioni o ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- divieto di compiere operazioni o impartire ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;

[7] Un apposito controllo automatico effettuato su base giornaliera dall'Unità Risk Management, con l'ausilio di un software fornito da una società esterna, evidenzia le operazioni ritenute potenzialmente sospette.

- divieto di compiere operazioni o ordini di compravendita che utilizzino artifizi o ogni altro tipo di inganno o di espediente;
- divieto di utilizzare altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda, o al prezzo di strumenti finanziari;
- divieto di trasmettere e revocare ripetutamente ordini di negoziazione, ove ciò possa ragionevolmente determinare una rilevante alterazione del prezzo dello strumento finanziario (es. per la dimensione, frequenza, tempistica e/o altre caratteristiche);
- divieto di porre in essere le condotte tipiche di manipolazione di mercato individuate dalle procedure/policy interne;
- divieto di accettare di eseguire un ordine impartito da un cliente se, al momento dell'acquisizione dell'ordine, vi sia la consapevolezza che tale esecuzione dia luogo al compimento di un reato o di un illecito amministrativo;
- obbligo di osservare le regole di comportamento ed i principi previsti dalla procedura "Market Sounding" in tema di partecipazione a sondaggi di mercato condotti da terzi.

L'iter procedurale previsto all'interno della SGR volto alla regolamentazione del processo relativo alla gestione e divulgazione delle informazioni e delle comunicazioni esterne, ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato, è basato sui seguenti presidi:

- abuso di informazioni privilegiate:
    - attivazione di una agenda degli incontri effettuati dagli appartenenti ai vari team di gestione e dagli analisti della SGR: mediante apposita funzione, è creato un report sintetico per ogni incontro avvenuto (tutte le informazioni inserite in agenda sono archiviate in apposito database)[8];
    - inserimento nell'agenda degli incontri di cui al bullet precedente, preventivamente agli stessi, delle seguenti informazioni:
        - data e ora incontro;
        - luogo dell'incontro;
        - estremi emittente/titolo oggetto dell'incontro;

[8] L'Unità Risk Management è responsabile della predisposizione di apposito report, indirizzato all'Organismo di Vigilanza, contenente tutte le informazioni utili al fine di controllare l'alimentazione dell'agenda degli incontri. Un controllo campionario sulla conformità dei contenuti degli incontri presenti nell'agenda degli incontri è effettuato dall'Unità Compliance, ogniqualvolta fosse necessario il compimento del "test del ragionevole sospetto", ovvero nel caso di operazione avente rilevanza informativa e\o in termini di ammontari negoziati.

    - inserimento nell'agenda degli incontri di cui al bullet precedente, successivamente all'incontro, delle seguenti informazioni:
        - partecipanti all'incontro;
        - argomenti discussi;
        - eventuale documentazione inerente l'incontro/l'emittente/titolo;
    - l'eventuale ricezione di informazioni privilegiate, ivi compresi i casi dubbi, è gestita sulla base dei principi sopra espressi così come è descritto l'iter procedurale conseguente (iscrizione nella "Restricted List" dell'emittente, blocco dell'operatività e suo monitoraggio);
- rapporti con la stampa:
    - autorizzazione preventiva, da parte dell'Amministratore Delegato, ai soggetti che rilasciano dichiarazioni, ovvero predispongono articoli;
    - controllo preventivo, da parte dell'Amministratore Delegato, sui contenuti degli articoli;
    - controllo successivo, da parte dell'Amministratore Delegato, sulle autorizzazioni rilasciate mediante riscontri sulla stampa.

L'iter procedurale previsto all'interno della SGR volto alla regolamentazione del processo relativo alla gestione delle operazioni di mercato, ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato, è basato sui seguenti presidi:

- predisposizione, da parte dei team di gestione, di report riassuntivi sulle motivazioni alla base delle scelte di investimento effettuate per conto dei portafogli gestiti;
- archiviazione dei sopracitati report e della eventuale documentazione a supporto delle scelte di investimento effettuate per conto dei portafogli gestiti;
- le operazioni che, a parere del singolo gestore, potrebbero ricadere nella fattispecie della manipolazione del mercato, anche se non presenti negli esempi forniti da MAR, dall'ESMA e Consob, e dall'Allegato I del MAR e dal Regolamento Delegato (UE) 2016/522, sono sottoposte all'attenzione del Responsabile dell'Unità Compliance;
- "test del ragionevole sospetto" e analisi delle delucidazioni fornite dai team di gestione sulle operazioni ritenute potenzialmente sospette (evidenziate grazie ad apposito software di controllo, nonché ai comunicati, provenienti dal motore di ricerca Google, inoltrati al Responsabile dell'Unità Compliance) effettuati da parte del Direttore Investimenti

\Responsabile Gestioni Individuali e, in seconda istanza, dal Responsabile dell'Unità Compliance.

Con riferimento all'attività ordinaria dei soggetti appartenenti alla Direzione Commerciale e alle Unità Consulenza, Trading Desk e RTO e Operations (Amministrazione Clienti), la Società ha adottato la propria "Policy Market Abuse", rivolta a tutti i dipendenti e a coloro che instaurano con la stessa rapporti di lavoro occasionale (ad es.: consulenti; collaboratori coordinati continuativi; collaboratori a progetto; stagisti, ecc...), nella quale sono state codificate le procedure ed i presidi organizzativi e di controllo che la Società ha inteso adottare al fine di prevenire la commissione di comportamenti rilevanti ai fini dell'applicazione della disciplina sull'abuso di informazioni privilegiate e sulla manipolazione del mercato, e di segnalare senza indugio a Consob le operazioni valutate come sospette.

In merito agli ordini/operazioni su strumenti finanziari ammessi alla negoziazione (o per i quali è stata presentata una richiesta di ammissione alle negoziazioni) in un mercato regolamentato italiano o di altro Paese dell'Unione Europea, o ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano, per i quali l'ammissione è stata richiesta o autorizzata dall'emittente, sono oggetto di monitoraggio le negoziazioni effettuate dalla Società per conto proprio (gestione della tesoreria), nonché le operazioni di ricezione e trasmissione di ordini della clientela.

Le disposizioni in materia di manipolazione di mercato trovano applicazione per ogni strumento finanziario ammesso alla negoziazione (o per il quale è stata presentata richiesta) in un mercato regolamentato di almeno uno Stato membro dell'Unione Europea, a prescindere dal fatto che le operazioni di negoziazione abbiano o meno effettivamente luogo in tale mercato. Pertanto, l'ambito di applicazione del processo di monitoraggio delle operazioni comprende anche le negoziazioni effettuate al di fuori dei mercati regolamentati (c.d. operazioni fuori mercato) o sui sistemi alternativi di negoziazione. Le operazioni fuori mercato rilevano ai fini della manipolazione anche quando non producono riflessi sui prezzi, sulla domanda o sull'offerta nel mercato regolamentato.

Inoltre, sono oggetto di costante monitoraggio anche dal punto di vista dell'abuso di mercato, le operazioni di compravendita di strumenti finanziari effettuate dai dipendenti e dai collaboratori della Società a titolo personale (c.d. personal dealing). Al fine di presidiare l'utilizzo improprio di informazioni privilegiate e, al contempo, monitorare l'ordinato svolgimento dell'attività aziendale, tutti i dipendenti e, più in generale, tutti i soggetti che, a vario titolo, operano in nome e/o per conto della Società (ad es.: consulenti; collaboratori coordinati continuativi; collaboratori a progetto;

stagisti; ecc.) devono attenersi scrupolosamente alle seguenti regole di comportamento. Chiunque venga, a qualunque titolo, a conoscenza di "informazioni privilegiate":

- deve astenersi dall'utilizzarle: sia qualora un eventuale impiego delle stesse vada a proprio personale vantaggio; sia nel caso in cui tale utilizzo possa arrecare un vantaggio a terzi; sia nel caso in cui il loro utilizzo possa favorire o determinare un vantaggio per la Società;
- deve darne tempestiva notizia al Responsabile dell'Unità Compliance che provvederà senza indugio ad iscrivere il titolo\emittente nella Restricted List;
- deve astenersi dal diffonderle all'interno e/o all'esterno della Società fuori dai casi in cui ciò sia strettamente necessario per il corretto e diligente adempimento delle proprie mansioni, da effettuarsi comunque nel rispetto dei previsti obblighi di legge.

Quando il responsabile o l'operatore delle strutture di Front Office individua, nell'esercizio delle proprie mansioni, un'operazione a suo giudizio qualificabile come "sospetta" sulla base degli elementi, circostanze, esempi e Indici di Anomalia previsti dalla vigente normativa e riportati nella "Policy Market Abuse", informa, con la massima sollecitudine e riservatezza, conservandone adeguata evidenza, il Responsabile dell'Unità Compliance, il quale, effettuate le verifiche di propria competenza, procede o meno all'inoltro della segnalazione.

Assumono in tale ambito particolare rilevanza le operazioni che saranno automaticamente rilevate dal Sistema di Detection della Società e che, ove non giustificate dal cliente, ovvero oggetto di comunicazione al pubblico (ad esempio in adempimento agli obblighi previsti in capo al cliente ai sensi della normativa sull'internal dealing), dovranno essere oggetto di segnalazione da parte della Funzione Risk Management al Responsabile della Funzione Compliance, per sue valutazioni (c.d. "test del ragionevole sospetto").

Il Responsabile dell'Unità Compliance analizza il singolo ordine/operazione e, se ne conferma il carattere sospetto, è tenuto a segnalarlo il primo possibile all'Amministratore Delegato che, a seguito di autonoma valutazione, invierà eventualmente la segnalazione alla Consob. Successivamente all'inoltro, copia della segnalazione viene archiviata a cura del Responsabile dell'Unità Compliance; in caso negativo, quest'ultimo procede all'archiviazione della pratica sottoposta all'istruttoria, indicandone la motivazione.

Qualora l'esame riguardi un ordine/operazione disposto/a da un soggetto o parte correlata dello stesso, coinvolto nel processo di verifica, l'interessato dovrà astenersi da ogni valutazione trasmettendo la pratica al successivo livello di controllo; nel caso in cui l'operazione in questione sia

riferibile all'Amministratore Delegato, la valutazione finale in merito all'opportunità di procedere ad effettuare la segnalazione spetterà al Presidente del Consiglio di Amministrazione.

Laddove un'operazione venga segnalata alla Consob, in relazione alle modalità di circolazione delle informazioni concernenti le operazioni sospette, si precisa che l'obbligo di riservatezza implica in capo al personale della Società:

- il divieto di informare soggetti terzi dell'avvenuta segnalazione, comprese le persone per conto delle quali le operazioni sono state eseguite (es. cliente, controparte), così come disposto dalla vigente normativa di riferimento;
- il divieto di diffusione di notizie all'interno della Società, ritenendosi inibita la possibilità di divulgare l'effettuazione della segnalazione anche al personale o ai collaboratori della stessa non interessati e/o coinvolti nell'operatività in oggetto, salvo il caso in cui l'operazione sia riferibile a più Unità oppure la valutazione del "carattere sospetto" dell'operazione comporti la necessità di coinvolgere altre Unità.

Le prescrizioni della "Policy Market Abuse" si intendono qui integralmente richiamate e costituiscono parte integrante del presidi di controllo e dei principi di comportamento anche nell'ottica della prevenzione delle condotte di abusi di mercato.

La Società ha altresì adottato una procedura "Ricezione e Trasmissione Ordini" avente lo scopo di definire le regole e le modalità operative per la ricezione e trasmissione di ordini di compravendita di strumenti finanziari provenienti dai Clienti al dettaglio e professionali. I destinatari del Modello sono tenuti ad attenersi a quanto disposto in materia di market abuse nella richiamata procedura. In particolare, gli appartenenti all'Unità Trading Desk e RTO, ricevute dalla Funzione Risk Management eventuali segnalazioni provenienti dal sistema di verifica del rispetto della normativa in materia di market abuse, forniscono tempestivamente ai responsabili delle Unità Risk Management e Compliance le spiegazioni afferenti le operazioni segnalate.

7.9. REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

La Legge 3 agosto 2007 n. 123 ha inserito nel D.Lgs. n. 231/2001 l'art. 25-septies che aggiunge all'elenco dei reati presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

7.9.1. FATTISPECIE DELITTUOSE

Le condotte di cui agli artt. 589 (omicidio colposo) e 590, comma 3 (lesioni personali colpose gravi o gravissime) c.p. consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima. Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

Ai sensi del predetto art. 25-septies del Decreto, entrambe le condotte devono essere caratterizzate dalla violazione delle norme dettate ai fini della prevenzione degli infortuni sul lavoro e sulla tutela dell'igiene e della salute sul lavoro.

Vengono a tal proposito in considerazione molteplici disposizioni, ora in gran parte confluite nel D.lgs. 9 aprile 2008, n. 81 a seguito dell'abrogazione da parte del medesimo di varie leggi speciali previgenti.

A completamento del corpo normativo delineato dalle specifiche misure di prevenzione prescritte dalle leggi in materia si colloca la più generale previsione di cui all'art. 2087 del codice civile, in forza del quale il datore di lavoro deve adottare le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie per tutelare l'integrità fisica e morale dei lavoratori.

Va infine tenuto presente che la giurisprudenza ritiene che i reati in questione siano imputabili al datore di lavoro anche qualora la persona offesa non sia un lavoratore, ma un estraneo, purché la sua presenza sul luogo di lavoro al momento dell'infortunio non abbia caratteri di anormalità ed eccezionalità.

7.9.2. ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i reati in tema di salute e sicurezza sul lavoro è la gestione degli adempimenti in materia di tutela della salute e della sicurezza sui luoghi di lavoro cui è tenuta la Società. Con riguardo alle fattispecie delittuose sopra individuate, le Unità organizzative principalmente coinvolte sono:

- Consiglio di Amministrazione;
- Amministratore Delegato;
- Unità Finanza.

In questo contesto, è opportuno segnalare che rientra nel rischio infortunio anche il c.d. rischio contagio nell'ambito della recente emergenza pandemica. Per questo, la Società ha integrato i propri presidi interni al fine di porre in essere tutte le misure – a cominicare dall'integrazione del DVR, l'adozione di uno specifico protocollo interno anti contagio e la nomina del c.d. Comitato per l'emergenza Covid – finalizzate alla prevenzione e alla gestione di questo particolare rischio infortunio, implementando gli specifici adempimenti richiesti dalla normativa di settore che si è susseguita nel tempo (cfr. i Protocolli condivisi Governo-Parti Sociali per la prevenzione del rischio Covid nelle imprese e i loro continui aggiornamenti). Tali misure, dunque, integrano a tutti gli effetti i protocolli 231 previsti dalla presente Parte Speciale.

7.9.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

In materia di organizzazione ai fini della sicurezza, la Società si è strutturata in modo tale da garantire un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

La struttura è analiticamente indicata nel documento di valutazione dei rischi, redatto ai sensi degli articoli 28 e 29 del D.lgs. 81/2008, che si intende integralmente richiamato nel Modello.

Il Datore di Lavoro è identificato nell'Amministratore Delegato; è stato nominato il Responsabile del Servizio di Prevenzione e Protezione, individuato in un soggetto dotato delle necessarie conoscenze e competenze tecniche; è inoltre stato nominato un Medico Competente per l'assolvimento degli obblighi di legge.

Il Modello, per la parte corrispondente ai reati in materia di salute e sicurezza sul lavoro, è stato formato facendo riferimento anche ai principi contenuti nel documento di valutazione dei rischi della Società.

I principi di comportamento qui di seguito individuati si applicano direttamente a chiunque sia tenuto, in via diretta od indiretta, all'osservanza delle norme antinfortunistiche.

È fatto espresso divieto di:

- porre in essere comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del Decreto);
- porre in essere comportamenti imprudenti, negligenti od imperiti che possano costituire un pericolo per la sicurezza all'interno del luogo di lavoro;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- svolgere attività lavorative in violazione delle disposizioni impartite dai responsabili per la sicurezza;
- svolgere attività lavorative senza aver preventivamente ricevuto adeguate istruzioni sulle modalità operative, oppure senza aver precedentemente partecipato a corsi di formazione.

Sotto l'aspetto generale, nell'ambito dei suddetti comportamenti i soggetti aziendali preposti all'attuazione delle misure di sicurezza - ciascuno per le attività di sua competenza specificamente individuate - sono tenuti ad assicurare:

- il rispetto degli standard tecnico-strutturali di legge;
- l'attuazione delle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- l'attuazione di modifiche di natura organizzativa finalizzate a far fronte a emergenze, primo soccorso, gestione degli appalti;
- il corretto svolgimento delle riunioni periodiche di sicurezza e delle consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- le attività di sorveglianza sanitaria;
- le attività di informazione e formazione dei lavoratori;

- le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- l'acquisizione della documentazioni e delle certificazioni obbligatorie di legge;
- le verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate.

Il Modello prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni o omissioni, conformemente alla loro formazione ed alle istruzioni e ai mezzi forniti dal Datore di Lavoro;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dal Responsabile per la sicurezza e dai soggetti preposti alla sicurezza ai fini della protezione collettiva ed individuale;
- segnalare immediatamente al Datore di Lavoro, al responsabile per la sicurezza o ai preposti alla sicurezza le deficienze dei mezzi e dispositivi a loro disposizione, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli;
- non rimuovere o modificare senza autorizzazione o comunque compromettere i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non siano di propria competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori;
- sottoporsi ai controlli sanitari previsti;
- contribuire, insieme al Datore di Lavoro, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

7.10. REATI INFORMATICI E IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

La Legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, fatta a Budapest il 23.11.2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi. La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D.Lgs. n. 231/2001 l'art. 24 bis, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli enti.

Nella medesima area di rischio vanno inquadrati anche i delitti in materia di violazione del diritto d'autore previsti dall'art. 25-novies del Decreto 231/01 (introdotto dalla legge 23 luglio 2009, n. 99): tale norma rende ascrivibili alla responsabilità degli enti una serie di reati previsti dalla Legge 633/41.

La trattazione in comune delle due tipologie criminose si giustifica in ragione del fatto che entrambe presuppongono l'utilizzo delle risorse informatiche e le attività "sensibili", così come i principi di controllo preventivo, sono in gran parte sovrapponibili.

7.10.1. FATTISPECIE DELITTUOSE

Si fornisce di seguito una descrizione delle fattispecie di reato di cui all'art. 24-bis del Decreto.

Accesso abusivo ad un sistema telematico o informatico (art. 615-ter c.p.)

Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici. Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse

pubblico o di fatti compiuti con abuso della qualità di operatore del sistema. Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della SGR (o anche di terzi concesse in licenza alla SGR), mediante l'utilizzo delle credenziali di altri colleghi abilitati.

Tale fattispecie di reato potrebbe configurarsi allorquando un destinatario del Modello o altro soggetto tenuto al rispetto del Modello abusivamente acceda (anche con l'ausilio del fornitore) al server di posta elettronica della Società, al fine di violare l'accesso alle caselle postali e-mail di altri soggetti ed utilizzare le informazioni ivi contenute nell'interesse della Società.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) e installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

La condotta punita dall'art. 617-quater c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni. L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. spyware). L'impedimento od interruzione delle comunicazioni (c.d. "Denial of service") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fasulle. Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema. Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall' installazione non autorizzata di un software da parte di un dipendente. L'art. 617-quinquies punisce il solo fatto della istallazione, fuori dai casi consentiti dalla legge, di apparecchiature atte a intercettare, impedire o interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

Tali fattispecie di reato si potrebbero configurare allorquando la SGR dovesse, direttamente o per interposta persona, intercettare comunicazioni relative ad un sistema informatico o telematico ovvero informazioni di terzi. Si ritengono tali fattispecie di remota applicazione presso la Società.

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) e danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)

L'art. 635 bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui. Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari. L'art. 635 ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità. Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio. Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p.

Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) e danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

L' art. 635-quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento. L'art. 635-quinquies c.p. punisce le medesime

condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità. In questa previsione, a differenza di quanto previsto all'art. 635 ter, non vi è più alcun riferimento all'utilizzo da parte di enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato, sufficiente l'utilizzo da parte di enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità. Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. E' da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento. Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p.

Le fattispecie di cui agli artt. 635-bis, 635-quater e 635-quinquies c.p. si individuerebbero laddove vi fosse un'attività da parte della SGR al fine di distruggere o deteriorare, cancellare informazioni di terzi. Si ritengono tali fattispecie di remota applicazione presso la Società.

La fattispecie di reato di cui all'art. 635-ter c.p. potrebbe configurarsi allorquando un destinatario del Modello o altro soggetto tenuto al rispetto del Modello abusivamente cancelli (anche con l'ausilio del fornitore) i dati contenuti in un programma informatico della Società al fine di sottrarli alla Pubblica Amministrazione (ad es. programmi di contabilità nell'ambito di un'ispezione fiscale).

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.) e diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

L'art. 615-quater punisce chiunque al fine di procurare a sé od ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo. L'art. 615-quinquies punisce chiunque si procura, produce, riproduce importa, diffonde, comunica consegna o mette a disposizione di altri apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema o i dati e i programmi ad

esso pertinenti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento. Tali fattispecie perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche. La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

La fattispecie di reato di cui all'art. 615-quater c.p. potrebbe configurarsi allorquando un destinatario del Modello o altro soggetto tenuto al rispetto del Modello abusivamente comunichi a terzi non autorizzati codici di accesso al server di posta elettronica della Società, al fine di violare l'accesso alle caselle postali e-mail di altri soggetti e utilizzare le informazioni ivi contenute nell'interesse della Società. Si ritiene, invece, la fattispecie di cui all'art. 615-quinquies c.p. di remota applicazione per la Società.

Falsità nei documenti informatici (art. 491-bis c.p.)

L'art. 491-bis c.p. dispone che ai documenti informatici pubblici o privati aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso. Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche. Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate. Con riferimento ai documenti informatici aventi efficacia probatoria, il falso

materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione. Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.). Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità. Tra i reati richiamati dall'art. 491 bis, sono punibili a querela della persona offesa la falsità in scrittura privata (art. 485 c.p.) e, se riguardano una scrittura privata, l'uso di atto falso (art. 489 c.p.) e la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

Tale fattispecie di reato potrebbe configurarsi allorquando, ad es., un destinatario del Modello o altro soggetto tenuto al rispetto del Modello non autorizzato utilizza (anche con l'ausilio del fornitore) la firma elettronica del legale rappresentante della Società, nell'interesse di questa, in violazione degli obblighi di custodia del relativo dispositivo.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)

Tale reato è commesso dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Il soggetto attivo del reato può essere evidentemente soltanto un soggetto "certificatore qualificato", che esercita particolari funzioni di certificazione per la firma elettronica qualificata. A tale specifico proposito si osserva che la SGR non riveste la qualifica di "certificatore qualificato" e che quindi tale disposizione non è di immediato interesse per la stessa. Si tenga comunque presente che – per assumere rilevanza penale – la violazione degli obblighi per il rilascio di un certificato qualificato deve essere assistita dal dolo specifico sopra evidenziato (perseguimento di un ingiusto profitto / danno altrui).

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019

Tale reato sanziona chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza

di cui al comma 6), lettera c) od omette di comunicare entro i temini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni.

Delitti in violazione del diritto d'autore e di altri diritti connessi al suo esercizio (artt. 171, 171-bis, 171-ter, 171-septies, 171-octies L.A.)

Si ritengono le fattispecie di cui agli artt. 171, 171-ter, 171-septies e 171-octies L.A. di remota applicazione per l'operatività della Società.

Si ritiene invece astrattamente configurabile in capo alla Società la fattispecie criminosa di cui all'art. 171-bis L.A., volto a tutelare il corretto utilizzo dei software e delle banche dati. Il reato può essere integrato attraverso una serie di condotte alternative, in particolare: (i) duplicazione abusiva di programmi per elaborare contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); o (ii) importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); o (iii) rimozione arbitraria o elusione di dispositivi applicati a protezione di un programma; o (iv) trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati; o (v) esecuzione dell'estrazione o del reimpiego della banca di dati; o (vi) distribuzione, vendita o concessione in locazione di una banca di dati.

7.10.2. ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Sebbene, da una parte, non si riscontrino attività specificamente sensibili rispetto alla commissione dei reati in esame – soprattutto in ragione del particolare ambito di attività nel quale la Società opera, che rende difficile ipotizzare la realizzazione di uno dei reati presupposto nell'interesse dell'ente –, d'altra parte ogni attività aziendale che utilizza tecnologie e risorse informatiche è potenzialmente esposta al rischio dei reati informatici e in materia di violazione di diritti d'autore. Tanto più che i reati informatici – o comunque realizzati attraverso i supporti informatici/telematici – possono essere realizzati con modalità tali da rendere oltremodo difficile la precisa individuazione dei soggetti (persone fisiche) autori dell'illecito e si prestano pertanto, in astratto, ad impegnare la responsabilità autonoma della Società, anche in caso di "autore non identificato", secondo la previsione normativa dell'art. 8 del Decreto 231/01.

Fermo restando, pertanto, che è l'utilizzo in sé delle risorse informatiche e telematiche a prestarsi ad un impiego distorto, abusivo ed illecito – potenzialmente rilevante ai sensi delle fattispecie qui in

esame – specifica rilevanza può essere attribuita alle seguenti attività "sensibili":

- gestione di comunicazioni e/o adempimenti per via telematica o utilizzando software pubblici;
- gestione di sistemi informativi aziendali o installazione, manutenzione, aggiornamento, gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici;
- gestione di sistemi informativi aziendali o installazione, manutenzione, aggiornamento o gestione di software e banche dati.

Con riguardo alle fattispecie delittuose sopra individuate, le Unità organizzative principalmente coinvolte sono:

- Direttore Finanza e Controllo;
- Unità Finanza;
- Unità Rapporti con le AA.VV.;
- Unità IT;
- chiunque utilizzi risorse informatiche/telematiche.

7.10.3.PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Al fine di prevenire la commissione delle fattispecie criminose previste dagli artt. 24-bis e 25–novies del Decreto 231/01, nonché allo scopo di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, adotta i seguenti principi di controllo e di comportamento, ai quali tutti i destinatari del Modello sono tassativamente tenuti a conformarsi:

- accesso al sistema informatico interno solo attraverso l'utilizzo di user-id e password personalizzate;
- periodico aggiornamento delle credenziali personali di accesso;
- limitazione dell'accesso al sistema informatico, attraverso abilitazioni differenziate, esclusivamente entro le finalità connesse alle specifiche funzioni svolte;
- utilizzo di strumenti di registrazione o di controllo delle operazioni compiute a mezzo di sistemi elettronici e/o informatici, in modo da poter avere sempre riscontro della correttezza delle procedure seguite e della coerenza interna delle varie fasi operative, nel rispetto dei limiti di cui alle norme vigenti;
- utilizzo di strumenti di tracciabilità degli accessi alle basi dati o a parti sensibili del software applicativo;

- informazione nei confronti del personale in merito al corretto utilizzo delle risorse informatiche aziendali;
- divieto di installazione e utilizzo di software non approvati dalla Società e non correlati con l'attività professionale svolta;
- divieto di installazione e utilizzo, sui sistemi informatici della Società, di software mediante i quali è possibile scambiare file con altri soggetti via internet, senza alcuna possibilità di controllo da parte della Società;
- predisposizione di un procedimento di autenticazione mediante username e password, limitato ad un numero limitato di soggetti abilitati, per l'accesso alle risorse di sistema;
- controllo aziendale periodico sulla rete informatica aziendale – nel rispetto della normativa sulla privacy e delle tutele lavorative e sindacali – allo scopo di individuare eventuali condotte anomale di soggetti apicali e dipendenti;
- controlli periodici funzionali alla verifica di corrispondenza tra le licenze e le banche dati in uso e quelle concordate con i fornitori dei relativi software;
- predisposizione di adeguate barriere fisiche di difesa e protezione dei server aziendali;
- informazione nei confronti del personale in merito al corretto utilizzo di materiale eventualmente protetto da diritto d'autore e, in particolare, in merito alla corretta modalità di selezione e utilizzo delle immagini anche in occasione della realizzazione di materiale pubblicitario o di presentazioni al pubblico;
- divieto di modificare la configurazione di postazioni di lavoro fisse o mobili;
- divieto di acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare traffico in transito etc.);
- divieto di ottenere o utilizzare credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;
- divieto di divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- divieto di accesso ad un sistema informatico altrui (anche di un collega) e manomettere o alterare i dati ivi contenuti;
- divieto di compromettere o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti;

- divieto di sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza di sistemi informatici o telematici di clienti o terze parti per ottenere o tentare di ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere;
- divieto di distorcere od oscurare la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati.

In ogni caso, il Responsabile dell'Unità IT ha l'obbligo di redigere e trasmettere annualmente all'Organismo di Vigilanza una dichiarazione attestante che, nel corso della verifica dell'integrità del sistema informatico aziendale, non sono state riscontrate manomissioni e/o anomalie.

La Società ha altresì adottato la procedura "Information Technology" – da intendersi qui integralmente richiamata -, che disciplina le modalità di utilizzo degli strumenti informatici e, più in generale, della dotazione resa disponibile dalla Società nell'ambito dello svolgimento delle proprie mansioni, dei propri compiti di lavoro e nelle attività di ufficio da parte dei dipendenti e del personale avente rapporti di collaborazione con la Società.

Le indicazioni fornite nella procedura sono da porsi in stretta relazione con le politiche di sicurezza che l'azienda adotta. Obiettivo ultimo della procedura è quello di tutelare la Società, i suoi dipendenti, i soci ed i clienti dalle conseguenze di azioni potenzialmente dannose e/o illegali commesse da qualsivoglia soggetto, con dolo o accidentalmente.

7.11. REATI TRIBUTARI

Il Decreto Legge 26 ottobre 2019, n. 124 ha introdotto all'interno del Decreto l'art. 25-quinquiesdecies, che estende la responsabilità amministrativa degli Enti in relazione ad un elenco di reati tributari disciplinati dal Decreto Legislativo 10 marzo 2000, n. 74 (di seguito, "D.Lgs. 74/2000"):

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, commi 1 e 2-bis, D.Lgs. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000);
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2-bis, D.Lgs. 74/2000);
- occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000);
- sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000).

Si tratta di reati direttamente lesivi di interessi fiscali, la cui introduzione si giustifica sia nell'ottica di un generale rafforzamento della lotta all'evasione fiscale sia nell'ambito dell'attuazione della Direttiva UE 2017/1371 (di seguito, "Direttiva PIF") relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione. Tale direttiva comunitaria demanda agli Stati Membri di prevedere la responsabilità delle persone giuridiche che abbiano tratto beneficio dalla consumazione di reati che ledono gli interessi finanziari dell'Unione, qualora tali reati siano stati commessi da parte dei membri apicali delle stesse, ovvero a seguito dell'omissione di controlli da parte dei vertici societari.

Il catalogo dei cosiddetti reati tributari che possono assurgere a reati presupposto della responsabilità amministrativa degli Enti è stato, poi, ulteriormente ampliato per effetto dell'emanazione del D.Lgs. 14 luglio 2020, n. 75, a mezzo del quale è stata ulteriormente recepita nell'ordinamento italiano la Direttiva PIF.

In particolare, è stato inserito all'interno dell'art. 25-quinquiesdecies del Decreto il comma 1-bis, ai sensi del quale possono costituire reati presupposto ai fini della disciplina di cui allo stesso Decreto anche le seguenti fattispecie delittuose:

- dichiarazione infedele (art. 4 D.Lgs. 74/2000);
- omessa dichiarazione (art. 5 D.Lgs. 74/2000);
- indebita compensazione (art. 10-quater D.Lgs. 74/2000),

e ciò a condizione che i predetti reati tributari siano stati commessi "nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro".

Sul punto va peraltro aggiunto che, in ottica prudenziale, le fattispecie di cui agli art. 4, 5 e 10-quater D.Lgs 74/2000, vengono considerate nel presente Modello potenzialmente rilevanti anche prescindendo dalla sussistenza delle condizioni di cui al comma 1-bis dell'art. 25-quinquiesdecies, ove integranti il reato fine di un reato associativo ovvero il reato presupposto, ad esempio, del reato di autoriciclaggio; per questa ragione, i protocolli specifici previsti nella presente parte speciale sono stati considerati e adottati anche contemplando tali ulteriori – seppur indiretti e certamente residuali – rischi reato.

Da ultimo, si evidenzia che ai sensi dell'art. 13-bis, comma 3, D.Lgs. 74/2000 "Le pene stabilite per i delitti di cui al titolo II sono aumentate della metà se il reato è commesso dal concorrente nell'esercizio dell'attività di consulenza fiscale svolta da un professionista o da un intermediario finanziario o bancario attraverso l'elaborazione o la commercializzazione di modelli di evasione fiscale".

7.11.1. FATTISPECIE DELITTUOSE

Si elencano di seguito le fattispecie contemplate dall'art. 25-quinquiesdecies del Decreto.

Dichiarazione fraudolenta mediante l'uso di fatture o altri documenti per operazioni inesistenti

Tale ipotesi di reato – prevista dall'art. 2, comma 1, del D.Lgs. 74/2000 – si configura nel caso in cui, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, vengano indicati elementi passivi fittizi in una delle dichiarazioni relative a dette imposte.

La condotta si caratterizza, quindi, come reato a dolo specifico di evasione la cui rilevanza prescinde dal raggiungimento di soglie quantitative di punibilità. È, tuttavia, prevista una sanzione pecuniaria di minore entità nel caso in cui l'ammontare degli elementi passivi fittizi sia inferiore a euro centomila, conformemente a quanto previsto dall'art. 2, comma 2-bis, del D.Lgs. 74/2000.

Ai sensi della norma in esame, per "fatture o altri documenti per operazioni inesistenti" devono intendersi fatture o documenti che siano registrati nelle scritture contabili obbligatorie ovvero siano detenuti a fini probatori nei confronti dell'amministrazione finanziaria.

Tale fattispecie ricorre, quindi, quando la dichiarazione resa all'amministrazione finanziaria, oltre ad essere non veritiera, è supportata da un "impianto" probatorio e documentale costituito allo scopo di sviare od ostacolare la successiva attività di accertamento dell'amministrazione finanziaria, o comunque ad avvalorare l'inveritiera prospettazione di dati in essa racchiusa.

Dichiarazione fraudolenta mediante altri artifici

Tale ipotesi di reato – prevista dall'art. 3 del D.Lgs. 74/2000 – si configura nel caso in cui, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni oggettivamente o soggettivamente simulate ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, si indichi in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi. Ai fini della rilevanza penale di tale condotta è necessario, tuttavia, che ricorrano congiuntamente le seguenti condizioni:

- l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila; e
- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore:
  - al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o comunque è superiore a euro un milione cinquecentomila; oppure
  - qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al 5% dell'ammontare dell'imposta medesima o comunque a euro trentamila.

A differenza, quindi, del reato di dichiarazione fraudolenta mediante l'uso di fatture o altri documenti per operazioni inesistenti, la punibilità del fatto resta subordinata al superamento di particolari soglie quantitative.

Ai fini dell'applicazione della fattispecie in esame:

- si considera commesso il fatto "avvalendosi di documenti falsi" quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria; e
- non costituiscono "mezzi fraudolenti" la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Emissione di fatture o altri documenti per operazioni inesistenti

Tale ipotesi di reato – prevista dall'art. 8, comma 1, del D.Lgs. 74/2000 - si configura quando, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, si emettano o si rilascino fatture o altri documenti per operazioni inesistenti.

Ai sensi dell'art. 8, comma 2-bis, del D.Lgs. 74/2000 è prevista una sanzione di minore entità qualora l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, sia inferiore a euro centomila.

Occultamento o distruzione di documenti contabili

Tale ipotesi di reato – prevista dall'art. 10 del D.Lgs. 74/2000 – si configura quando, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, si occultino o si distruggano in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Per tale fattispecie di reato non è prevista alcuna soglia minima di punibilità.

Sottrazione fraudolenta al pagamento di imposte

Tale ipotesi di reato – prevista dall'art. 11 del D.Lgs. 74/2000 – contempla due differenti fattispecie, ed in particolare:

- il caso in cui, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, si alieni simulatamente o si compiano altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva;
- il caso in cui, al fine di ottenere per sè o per altri un pagamento parziale dei tributi e relativi accessori, si indichi nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

Si noti che la rilevanza penale della condotta non è data dal mero inadempimento dell'obbligazione pecuniaria avente ad oggetto l'imposta ed i relativi accessori, bensì dalle condotte fraudolente che la precedono.

Dichiarazione infedele

La fattispecie di reato in esame si configura, salvo che non ricorrano i presupposti per ritenere integrate le più gravi fattispecie delittuose di cui agli artt. 2 e 3 del D.Lgs. 74/2000, allorché un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative alle predette imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti. Perché si possa ritenere integrata la fattispecie delittuosa in esame è necessario, sempre in linea generale, il superamento di una duplice soglia di punibilità. E', infatti, richiesto che:

- l'imposta evasa sia superiore, con riferimento alle singole imposte, a euro centomila; e
- l'ammontare complessivo degli elementi attivi sottratti a imposizione, anche per effetto dell'indicazione in dichiarazione di elementi passivi inesistenti, sia superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o, in ogni caso, a euro due milioni.

L'art. 4, comma 1-bis, D.Lgs. 74/2000 prevede che, ai fini della configurazione del reato di dichiarazione infedele non si tiene conto della non corretta classificazione e valutazione di elementi attivi o passivi oggettivamente esistenti, con riferimento ai quali i criteri di classificazione e valutazione concretamente adottati sono stati indicati in bilancio o in altri documenti aventi rilevanza ai fini fiscali, nonché, della violazione di principi di competenza, non inerenza o dell'indeducibilità di elementi passivi reali.

L'art. 4, comma 1-ter, D.Lgs. 74/2000 dispone che non danno luogo a fattispecie aventi rilevanza penale le valutazioni che complessivamente considerate differiscono da quelle corrette in misura inferiore al 10%.

Ciò posto in termini generali con riferimento agli elementi costitutivi del delitto di dichiarazione infedele, si rileva che l'art. 25-quinquiesdecies, comma 1-bis, del Decreto prevede che il reato tributario in esame rileva come reato presupposto ai fini della configurabilità di un'ipotesi di responsabilità amministrativa ai sensi dello stesso Decreto esclusivamente nell'ipotesi in cui sia stato commesso "nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro".

Omessa dichiarazione

La fattispecie in oggetto si configura allorché un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, pur essendo gravato da uno specifico obbligo in tal senso, una delle dichiarazioni relative alle predette imposte.

Al fine di ritenere integrata la fattispecie delittuosa in esame è necessario, in linea generale, il superamento di una soglia di punibilità. Ed infatti, è richiesto che l'imposta evasa risulti essere superiore, con riferimento a ciascuna imposta considerata dalla norma, a euro cinquantamila.

L'art. 5, comma 1-bis, del D.Lgs. n. 74/2000 attribuisce rilevanza penale anche alla condotta del soggetto che omette, pur essendovi obbligato, di presentare la dichiarazione di sostituto di imposta; e ciò a condizione che l'ammontare delle ritenute non versate ecceda l'importo di euro cinquantamila (soglia di punibilità).

Ciò posto in termini generali con riferimento agli elementi costitutivi del delitto di omessa dichiarazione, si rileva che l'art. 25-quinquiesdecies, comma 1-bis, del Decreto prevede, anche in questo caso, che il reato tributario in esame rileva come reato presupposto ai fini della configurabilità di un'ipotesi di responsabilità amministrativa ai sensi dello stesso Decreto esclusivamente nell'ipotesi in cui sia stato commesso "nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro".

Indebita compensazione

La fattispecie in esame punisce colui che "non versa le somme dovute" utilizzando in compensazione, ai sensi dell'art. 17 del D.Lgs. 9 luglio 1997, n. 241, crediti non spettanti per un importo annuo superiore a euro cinquantamila.

L'art. 10-quater, comma 2, del D.Lgs. 74/2000 prevede una circostanza aggravante che risulta essere integrata qualora venga utilizzato indebitamente in compensazione, ai sensi dell'art. 17 del D.Lgs. 9 luglio 1997, n. 241, un credito inesistente.

Ciò posto in termini generali con riferimento agli elementi costitutivi del delitto di indebita compensazione, si rileva che l'art. 25-quinquiesdecies, comma 1-bis, del Decreto prevede, anche in questo caso, che il reato tributario in esame rileva come reato presupposto ai fini della configurabilità di un'ipotesi di responsabilità amministrativa ai sensi dello stesso Decreto esclusivamente nell'ipotesi in cui sia stato commesso "nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro".

7.11.2. ATTIVITÀ AZIENDALI SENSIBILI E UNITÀ ORGANIZZATIVE COINVOLTE

Le attività "sensibili" identificate dal Modello, nelle quali è maggiore il rischio che siano posti in essere reati tributari, possono essere suddivise in attività suscettibili di dar luogo a rischi "diretti" di commissione di reati tributari, a rischi "di concorso" nella commissione di reati tributari e a rischi "indiretti" di commissione di reati tributari. Tali attività sono le seguenti:

Rischi "diretti"

- gestione degli adempimenti fiscali;
- emissione di fatture (ciclo attivo);
- tenuta e conservazione delle scritture contabili;
- M&A e Operazioni straordinarie della Società;
- Lancio di nuovi prodotti e creazione di fondi all'estero;

Rischi "di concorso"

- gestione degli adempimenti fiscali legati ai prodotti gestiti;
- attività di consulenza nell'interesse dei client (anche in relazione a eventuali trust, fondi patrimoniali, etc.).

Rischi "indiretti"

- acquisto di beni e servizi (ciclo passivo);
- contabilità e bilancio;
- rapporti infragruppo;
- gestione fiscale degli eventi promozionali, delle sponsorizzazioni e donazioni (compresi i rapporti con ONLUS del gruppo);
- gestione delle risorse finanziarie e della tesoreria;
- gestione delle risorse umane (ad es. selezione, assunzione, amministrazione, valutazione, etc.) e delle note spese;

In particolare, con riguardo alle fattispecie delittuose in esame, le possibili modalità di realizzazione delle condotte sono:

- rispetto ai reati di cui agli artt. 2, 3 e 8 del D.Lgs. 74/2000, l'emissione di fatture o altri documenti per operazioni inesistenti e/o la presentazione di dichiarazioni fraudolente/infedeli. Tale condotta potrebbe configurarsi anche nell'ambito dei rapporti con altre società del gruppo di appartenenza della SGR in relazione ai servizi prestati o ricevuti sulla base di specifici contratti di prestazione di servizi infragruppo sottoscritti dalle parti;
- rispetto al reato di cui all'art. 10 del D.Lgs. 74/2000, l'occultamento o la distruzione in tutto o in parte delle scritture contabili o dei documenti di cui è obbligatoria la conservazione secondo la normativa fiscale o civilistica italiana, rendendo impossibile la ricostruzione del proprio reddito;
- inoltre, la Società potrebbe, a titolo di concorso nel reato fiscale perpetrato dai propri clienti, agevolare la realizzazione del reato dichiarativo del cliente consentendo consapevolmente allo stesso un indebito e fraudolento abbassamento dell'imponibile fiscale relativo alle imposte sui redditi, attraverso ad esempio la fornitura di falsi documenti relativi ai prodotti gestiti, l'occultamento o la distruzione in tutto o in parte delle scritture contabili o dei documenti di cui è obbligatoria la conservazione secondo la normativa fiscale o civilistica italiana, rendendo impossibile la ricostruzione del reddito del cliente, nonché l'implementazione di strutture quali trust e fondi patrimoniali finalizzati alla sottrazione del patrimonio del cliente al pagamento delle imposte integrando la fattispecie prevista dall'art. 11 del D.Lgs. 74/2000;
- infine, in relazione alle fattispecie di cui agli artt. 4 e 5, vanno considerati innanzitutto tutti qui rapporti di acquisto e di vendita con controparti straniere che abbiano un impatto rilevante sull'IVA che la Società è tenuta a versare; ciò anche laddove la controparte sia una società del Gruppo. Inoltre, si ritengono comunque esposte a tali rischi reato (in connessione con rischi reato associativi o di autoriciclaggio, per quanto sopra precisato) le attività di strutturazione all'estero di fondi nella cui gestione svolga un ruolo anche personale della Società e le operazioni straordinarie all'estero che abbiano possibili impatti fiscali. Allo stesso modo, si ritiene comunque prudente considerare quale attività esposta alla fattispecie tipica "base" dei reati di cui agli art. 4 e 5 D.Lgs 74/00 (dunque anche in assenza delle condizioni di cui al comma 1-bis dell'art. 25-quinquiesdecies), la generale gestione della fiscalità e della contabilità sottostante della Società.

Con riguardo alle fattispecie delittuose sopra individuate, i soggetti\le Unità organizzative principalmente coinvolte sono:

- Consiglio di Amministrazione;
- Amministratore Delegato;

- Direttore Finanza e Controllo;
- Unità Affari Legali e Societari;
- Direzione Commerciale;
- Unità Operations;
- Unità Finanza;
- Unità Analisi di Gestione;
- Unità IT;
- Comitato Remunerazioni;
- Unità Risk Management;
- Project leader.

7.11.3. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO E PROTOCOLLO AZIENDALE

Al fine di presidiare il rischio di commissione dei reati tributari sopra individuati, sono stati adottati specifici presidi a livello di gruppo e di Società.

L'attività di prevenzione si basa sull'adozione di un sistema di controlli articolato, con compiti specifici e differenziati, nonché su policy e procedure interne che si possono suddividere a seconda che si riferiscano ad attività suscettibili di dar luogo a rischi "diretti" di commissione di reati tributari, a rischi "di concorso" nella commissione di reati tributari e a rischi "indiretti" di commissione di reati tributari.

Rischi "diretti"

Il principale rischio "diretto" di commissione di reati tributari concerne l'attività di gestione degli adempimenti fiscali della Società.

Con riferimento alla fiscalità propria della Società, la procedura da porre in essere nello svolgimento degli adempimenti previsti per il rispetto della normativa in materia fiscale è coordinata e messa in atto dall'Unità Finanza, anche attraverso l'ausilio di soggetti esterni quali una società per la parte di conformità, un consulente fiscale e una Società di Revisione.

Prima di passare in rassegna i principali adempimenti fiscali e le relative procedure adottate dalla Società, occorre innanzitutto rilevare che le principali attività svolte dalla stessa sono l'attività di gestione di fondi comuni di investimento, caratterizzata dal regime di esenzione ai fini IVA, e il servizio di gestione patrimoniale e di consulenza, soggetto ad IVA. A partire dal 1° gennaio 2013, la Società ha

adottato il regime IVA misto per tutte le attività ai sensi dell'articolo n. 36-bis del D.P.R. n. 633/72, che prevede la dispensa da alcuni adempimenti amministrativi e fiscali per le operazioni esenti, nel caso di ricavi percepiti dalla Società da parte della clientela, e pertanto, a fronte dell'indetraibilità dell'IVA sugli acquisti, l'obbligo di emissione della fattura attiva non sussiste, fatta eccezione per il caso in cui sia il cliente a farne esplicita richiesta. Fanno eccezione a tale regime "semplificato" le attività relative al servizio di gestione patrimoniale e di consulenza, per le quali si applica il regime IVA ordinario.

Si sintetizzano di seguito i principali adempimenti fiscali e le relative policy della Società, illustrate in modo completo e dettagliato nella procedura aziendale denominata "Adempimenti fiscali", a cui si fa espresso rinvio:

- tenuta dei libri obbligatori IVA: la tenuta dei libri obbligatori ai fini IVA è eseguita da una persona addetta nell'ambito dell'Unità Finanza;
- liquidazione mensile dell'IVA: l'addetto dell'Unità Finanza compila il modello F24 e, a seguito di controllo di merito da parte del responsabile dell'Unità, raccoglie le firme e lo invia alla società di compliance che si occupa dell'invio telematico;
- comunicazioni periodiche dati IVA: l'addetto dell'Unità Finanza invia al consulente fiscale le risultanze della procedura di liquidazione IVA per la predisposizione della comunicazione periodica del trimestre di riferimento in anticipo sulla scadenza normativamente prevista per la trasmissione, il riepilogo IVA acquisti, il riepilogo IVA vendite ed il riepilogo dei registri dei corrispettivi nonché tutti i modelli F24 da cui si evincono i versamenti effettuati nel corso del trimestre oggetto di comunicazione. Il consulente fiscale provvede quindi a predisporre la comunicazione trimestrale di riferimento e, a seguito di controllo di merito da parte dell'Unità Finanza, provvede alla trasmissione in forma telematica agli Uffici competenti, rilasciando all'Unità Finanza copia della documentazione comprovante l'invio della comunicazione ed il ricevimento da parte degli Uffici competenti;
- dichiarazione annuale IVA: il consulente fiscale provvede a predisporre la dichiarazione annuale sulla base dei dati e della documentazione di cui è già in possesso in quanto utilizzati per la predisposizione delle comunicazioni trimestrali dei dati IVA di cui al punto precedente e, a seguito di controllo di merito da parte dell'Unità Finanza, provvede alla trasmissione in forma telematica agli Uffici competenti entro la scadenza normativamente prevista per la trasmissione, rilasciando all'Unità Finanza, copia della documentazione comprovante l'invio della dichiarazione ed il ricevimento da parte degli Uffici competenti;

- operazioni intracomunitarie: il modello Intrastat contenente gli elenchi delle operazioni intra-comunitarie viene compilato con cadenza mensile, con il supporto della società di compliance, sulla base delle evidenze documentali predisposte dall'Unità Finanza e verificato (e firmato) dal responsabile dell'Unità. L'invio telematico del Modello Intrastat è effettuato, entro e non oltre il giorno 25 di ogni mese, dalla società di compliance che provvede, altresì, alla trasmissione all'Unità Finanza della documentazione comprovante l'invio;
- certificazioni delle ritenute d'acconto: l'Unità Finanza provvede a predisporre, all'atto del pagamento di fatture con applicazione della ritenuta d'acconto, un prospetto, redatto in formato excel, dove sono riportati tutti i dati necessari ed opportuni alla predisposizione delle certificazioni delle ritenute d'acconto operate sulle prestazioni professionali rese dai liberi professionisti. L'Unità Finanza invia il suddetto prospetto alla società di compliance in anticipo rispetto della scadenza normativamente prevista per l'invio di tali certificazioni. Precedentemente all'invio, l'Unità Finanza effettua gli opportuni controlli e la quadratura con i versamenti effettuati nel corso dell'anno ed i relativi modelli F24. Sulla base del prospetto ricevuto, la società di compliance predispone le bozze di certificazioni e le invia, a mezzo posta elettronica, all'Unità Finanza, con un congruo anticipo rispetto alla scadenza normativamente prevista, in modo da consentire all'Unità Finanza di effettuare i controlli finali di corrispondenza di quanto riportato nelle lettere di certificazione con i dati indicati nel prospetto utilizzato per la loro redazione. Conclusi i controlli di propria competenza, l'Unità Finanza provvede a trasmettere le certificazioni all'Unità Segreteria che si occupa dell'invio delle stesse alle controparti coinvolte;
- presentazione del Modello Unico: l'Unità Finanza trasmette al consulente fiscale copia del conto economico della Società al 31 dicembre dell'esercizio il cui reddito deve essere assoggettato a tassazione, nonché tutta la documentazione e le informazioni necessarie per classificare correttamente le componenti reddituali al fine di individuare le variazioni in aumento ed in diminuzione e quindi di determinare da ultimo il reddito imponibile. In base alla documentazione ricevuta, il consulente fiscale determina le imposte dell'esercizio e le eventuali imposte anticipate e/o differite secondo la normativa fiscale di volta in volta applicabile nonchè predispone la bozza del Modello Unico che trasmette all'Unità Finanza in congruo anticipo rispetto ai tempi previsti dalla normativa vigente per l'invio del Modello Unico, affinchè la stessa possa procedere ai controlli di merito sulla correttezza e completezza del Modello. Conclusi i controlli di propria competenza e le verifiche di merito con il responsabile dell'Unità Finanza, l'Unità Finanza sottopone le risultanze alla Società di Revisione al fine di condividerne preliminarmente i contenuti. Il Modello Unico, sottoscritto in tre copie originali dal legale rappresentante della

Società e della Società di Revisione, è trasmesso al consulente fiscale che, apposta la propria firma in qualità di intermediario abilitato all'invio in forma telematica del modello, provvede alla trasmissione dello stesso all'Agenzia delle Entrate entro i termini previsti dalla normativa di volta in volta vigente;

- prezzi di trasferimento: la Società, con l'ausilio di un consulente fiscale, redige la documentazione di cui all'art. 1, comma 2-ter, del D.Lgs. N. 471/1997, idonea a consentire il riscontro della rispondenza al principio di libera concorrenza dei prezzi di trasferimento praticati dalle imprese multinazionali. In particolare, l'Unità Finanza trasmette al consulente fiscale tutta la documentazione necessaria per effettuare l'analisi economica delle transazioni intragruppo cross border unitamente al bilancio d'esercizio ed alla documentazione contrattuale sottostante ai rapporti intragruppo in essere. L'Unità Finanza si occupa di redigere la descrizione generale della Società, dei settori in cui essa opera, della struttura operativa della stessa e delle strategie generali perseguite mentre il consulente fiscale fornisce consulenza e supporto nella stesura della descrizione e dell'analisi economica delle transazioni internazionali che la Società pone in essere con le consociate estere. Predisposto il documento finale ed effettuati i controlli incrociati sullo stesso, la Documentazione Nazionale è sottoscritta dal Responsabile dell'Unità Finanza entro i termini previsti per la presentazione del Modello Unico ed è archiviata, insieme a tutta la documentazione utilizzata, dal consulente fiscale. Si evidenzia che per quanto concerne la materia del transfer pricing la Società ha inoltre adottato una specifica policy denominata "Prezzi di trasferimento per transazioni infragruppo";
- oltre ai citati presidi specifici, sono previste apposite attestazioni, da parte dei responsabili delle funzioni aziendali, verso le competenti funzioni amministrative circa: (i) la completa, corretta e tempestiva informazione dei fatti riguardanti la Società; (ii) le rilevazioni contabili delle operazioni riguardanti la Società eseguite nel rispetto dei principi di inerenza, competenza e documentazione; (iii) non si è a conoscenza di altre informazioni e dati che possano avere rilevanza ai fini della corretta e completa rappresentazione della situazione economica e patrimoniale della Società e del risultato ante imposte sulla cui base svolgere il calcolo delle stesse;
- infine, il Direttore Finanza e Controllo è responsabile di curare l'aggiornamento formativo in materia fiscale della propria funzione e di tutti gli esponenti aziendali che ricoprono un ruolo nel processo di gestione degli adempimenti fiscali; a tal fine, si avvale del contributo del consulente fiscalista, espressamente incaricato, per l'invio di newsletter e la tenuta di corsi di aggiornamento in casi di novità rilevanti.

Ulteriori rischi “diretti” di commissione di reati tributari possono concernere l’attività di emissione di fatture (ciclo attivo) e l’attività di tenuta e conservazione delle scritture contabili.

Per quanto concerne l’attività di emissione di fatture (ciclo attivo), la Società ha adottato la procedura “Contabilità e bilancio”, a cui si fa espresso rinvio. In particolare, nella sezione “Ciclo attivo (Clienti)” sono descritte le modalità di gestione e contabilizzazione delle fatture attive emesse a clienti della Società e delle commissioni attive percepite dalla Società in relazione allo svolgimento del servizio di gestione patrimoniale e dell'attività di gestione collettiva, potendosi distinguere le seguenti principali categorie di fatture: fatture relative ai servizi intercompany, fatture relative al servizio di consulenza (advisory), fatture relative al servizio di custodia e amministrazione, fatture relative al servizio di collocamento, fatture relative all’eventuale dismissione/cessione di beni aziendali, fatture relative al servizio di gestione patrimoniale.

La procedura interna prevede uno stringente insieme di regole a garanzia della piena regolarità e correttezza delle fatture attive emesse per le attività svolte dalla Società.

Innanzitutto, è attribuito all’Unità Operations il compito di censire l’anagrafica di ogni cliente nell’apposito sistema gestionale in uso che attribuisce ad ogni cliente un codice identificativo di tutti i suoi rapporti verso la Società.

La periodicità della fatturazione varia a seconda dell’attività cui si riferisce. Per cui, ad esempio, le fatture relative ai servizi intercompany vengono emesse periodicamente in base alle previsioni contrattuali ed inviate alle società del gruppo accompagnate da una lettera, che descrive nel dettaglio i servizi fatturati. Gli importi delle suddette fatture vengono predisposti sulla base delle indicazioni fornite dall'Unità Analisi di Gestione. Le fatture relative alla dismissione/cessione di beni aziendali, vengono emesse nei casi eccezionali di vendita a clienti e/o dipendenti di beni/cespiti aziendali. Le fatture riferite all’attività di collocamento svolta dalla Società vengono emesse periodicamente in base alle previsioni contrattuali. Le fatture relative agli altri servizi di investimento forniti alla clientela sono prodotte in modo automatico dal sistema gestionale, sulla base delle commissioni attive maturate nei confronti della clientela. La periodicità di fatturazione dipende altresì dalla tipologia di servizio, potendo essere mensile o trimestrale. L’Unità Finanza provvede a stampare le suddette fatture che, a seguito del controllo di correttezza dell’importo, sono poi inviate alla clientela.

Le fatture sono sempre stampate su carta intestata in duplice copia. Una copia è registrata nel sistema di contabilità generale ed archiviata; l'altra copia viene inviata al cliente.

Tutte le fatture sono annotate sul registro delle vendite. La stampa dei registri è effettuata in versione provvisoria trimestralmente ed in formato definitivo annualmente entro e non oltre il secondo mese successivo dell'anno nella cui dichiarazione c'è l'obbligo del versamento della relativa IVA. Tutti i registri e le fatture dell'esercizio in corso e di quelli precedenti sono attualmente archiviati presso l'Unità Finanza sulla base della procedura di archiviazione della Società.

Regole specifiche sono poi previste per la contabilizzazione delle commissioni attive relative all'attività di gestione collettiva del risparmio, sono descritte nel dettaglio nella citata procedura "Contabilità e bilancio".

Infine, la procedura in esame prevede anche un sistema di controlli e archiviazione della fatturazione attiva. In particolare, la persona incaricata svolge gli opportuni controlli sulle attività di contabilità generale e gli adempimenti ad essa connessi, in modo da evitare errori e il rischio di sanzioni di carattere amministrativo e/o penale.

Per quanto concerne l'attività di tenuta e conservazione delle scritture contabili, la Società ha adottato la policy "Gestione archivio documentale", a cui si fa espresso rinvio, oltre alla già citata procedura "Contabilità e bilancio".

Le disposizioni della policy "Gestione archivio documentale" riguardano l'archiviazione dei documenti che necessitano di essere conservati nel tempo e prevedono stringenti regole relative all'individuazione di un soggetto responsabile per la corretta e tempestiva archiviazione dei documenti nonchè dei responsabili di ciascuna unità incaricati garantire che la documentazione della propria unità sia archiviata, all'esternalizzazione del servizio di archiviazione dei documenti, alle modalità di conservazione dei documenti e, infine, all'accesso ai documenti archiviati. Sempre in tema di contabilità e bilancio, ai citati presidi si aggiungono i protocolli specifici previsti nel presente Modello nella Parte Speciale dedicata ai Reati societari, a cui si rinvia.

Per quanto concerne le operazioni di M&A e operazioni straordinarie aventi potenziali effetti fiscali, la Società ha adottato i seguenti protocolli:

- il responsabile della funzione proponente l'operazione, individuata alla luce del sistema di deleghe e procure, predispone idonea documentazione a supporto dell'operazione proposta, nonché una relazione informativa preliminare che illustri i contenuti, l'interesse sottostante e le finalità strategiche dell'operazione;
- il Consiglio di Amministrazione, prima di autorizzare per iscritto l'operazione, verifica la sussistenza dei presupposti di carattere strategico, economico e finanziario nonché di attuabilità della proposta;
- il Direttore Finanza e Controllo verifica la corrispondenza tra la proposta dell'operazione autorizzata e i contenuti del contratto cui si è pervenuti a seguito delle attività negoziali; ogni modifica del contratto rispetto alla proposta è autorizzata preventivamente dal Consiglio di Amministrazione;
- l'operazione straordinaria è sempre comunque comunicata, ove previsto dalla normativa vigente, all'Autorità di Vigilanza secondo disposizioni di legge e di questa informativa è tenuta traccia documentale;
- il Direttore Finanza e Controllo, anche avvalendosi dell'outsourcer tributario, effettua una due diligence fiscale in relazione ad ogni operazione straordinaria, tenendo traccia dell'esito delle verifiche;
- ai fini della registrazione contabile dell'operazione, il Direttore Finanza e Controllo verifica preliminarmente la completezza, l'inerenza e la correttezza della documentazione di supporto dell'operazione;
- tutta la documentazione relativa all'operazione è archiviata a cura del Direttore Finanza e Controllo.

Per quanto riguarda il lancio di nuovi prodotti e la creazione di nuovi fondi all'estero, si applica la procedura "Nuovi Prodotti\Servizi" che regola le singole fase di strutturazione e approvazione dei nuovi prodotti, i connessi passaggi autorizzativi, le funzioni coinvolte, la tracciabilità delle singole fasi. Inoltre, è sempre effettuato preventivamente un assessment fiscale, richiesto dal Consiglio di Amministrazione, affinché si valutino gli impatti fiscali e i connessi oneri relativi al nuovo fondo che ricadono sulla Società, integrando a tal fine e di conseguenza la proceduray "Processo di valorizzazione" nella sezione "Oneri fiscali".

Sia nel caso di creazione di nuove branch o società collegate, sia nel caso di creazione all'estero di nuovi fondi, è essenziale applicare anche i seguenti protocolli generali:

a) la gestione della nuova realtà societaria o del nuovo fondo deve essere coerente con il Paese ove hanno la sede;

b) la nuova realtà societaria e il nuovo fondo devono essere dotati della struttura societaria e organizzativa perché possano essere gestiti nel luogo in cui hanno sede.

Infine, laddove i sopra citati protocolli – in relazione a tutti i "Rischi diretti" oggetto della presente sezione – prevedano l'intervento di un consulente fiscalista esterno, il rapporto tra la Società e il consulente è regolato dai protocolli previsti in tema di acquisto di beni e servizi, a cui si rinvia.

Rischi "di concorso"

La Società potrebbe in linea di principio concorrere in reati fiscali perpetrati dai propri clienti quali i reati dichiarativi, oppure il reato di sottrazione del patrimonio del cliente al pagamento delle imposte. Le attività maggiormente esposte a tali rischi sono l'attività di gestione degli adempimenti fiscali legati ai prodotti gestiti e l'attività di consulenza nell'interesse dei clienti (anche in relazione a eventuali trust, fondi patrimoniali, ecc.).
Sotto il primo profilo, la Società ha inserito nella procedura "Processo di valorizzazione", a cui si fa espresso rinvio, una sezione denominata "Oneri Fiscali", nella quale sono descritte le procedure relative alla gestione degli adempimenti fiscali legati ai prodotti gestiti.
Inoltre, ad ulteriore presidio della corretta operatività nell'ambito delle attività aziendali sensibili sono state adottate dalla Società specifiche regole di comportamento in materia di rapporti con la clientela illustrate in modo completo e dettagliato nelle policy "Codice di condotta in materia fiscale" e "Foreign Account Tax Compliance ACT (FATCA) e Qualified Intermediary (QI)" e "Common Reporting Standard", nonché nel "Manuale Qualified Intermediary Agreement".
Si tratta di regole finalizzate a garantire il rispetto della normativa (anche) fiscale da parte della Società e dei suoi clienti, ad assicurare il corretto adempimento degli obblighi di comunicazione e segnalazione rilevanti in sede internazionale e, quindi, a presidiare il rischio di commissione di reati fiscali.

Le procedure e i protocolli in esame disciplinano i rapporti della Società – non solo – con i propri clienti, bensì anche con gli eventuali titolari effettivi nel caso di clienti entità giuridiche (vale a dire di posizioni intestate a soggetti diversi dalle persone fisiche), scongiurando in tal modo qualsivoglia aggiramento degli obblighi ivi previsti.

In maggior dettaglio, per quanto riguarda le regole del "Codice di condotta in materia fiscale", non devono essere aperte relazioni con nuovi clienti qualora la Società abbia una notizia tale da far presupporre che il potenziale cliente non abbia adempiuto ai propri obblighi fiscali nel paese in cui risiede fiscalmente, né nuovi conferimenti verso conti esistenti devono essere accettati se esistono elementi che portino a ritenere che i valori conferiti siano legati a frodi fiscali. Inoltre, fermo restando l'obbligo di adeguata verifica del cliente con il quale la Società instaura un rapporto, nel caso in cui dovessero essere identificati degli indizi di possibili reati fiscali, l'Unità Compliance deve essere tempestivamente informata al fine di svolgere un'analisi più approfondita. L'eventuale violazione del presente codice potrebbe comportare sanzioni o provvedimenti disciplinari.

Per quanto riguarda le regole contenute nel "Foreign Account Tax Compliance ACT (FATCA) e Qualified Intermediary (QI)" e nel "Manuale Qualified Intermediary Agreement", vengono descritti i principali adempimenti, i ruoli e le responsabilità, al fine di assicurare la conformità con le normative FATCA e QI.

Il regime FATCA/QI prevede quali principali adempimenti l'identificazione e documentazione di tutti i conti detenuti da persone fisiche e giuridiche, al fine di determinare se siano o meno statunitensi, e la comunicazione all'Agenzia delle Entrate, la quale comunicherà all'IRS le informazioni riguardanti la clientela statunitense.

Per quanto riguarda le regole contenute nel "Common Reporting Standard", vengono descritti i principali adempimenti, i ruoli e le responsabilità, al fine di assicurare la conformità con la normativa CRS.

Il regime CRS prevede quali principali adempimenti, l'identificazione e documentazione di tutte le persone fisiche e giuridiche che detengono attività finanziarie al di fuori della propria giurisdizione di residenza fiscale e la comunicazione all'Agenzia delle Entrate, la quale scambierà le informazioni con l'autorità fiscale competente nella giurisdizione fiscale degli stessi clienti.

Ai fini di cui sopra, la Società si è dotata di una procedura di due diligence volta ad adempiere agli obblighi FATCA e CRS.

In ogni caso, è fatto generale divieto, a qualsiasi struttura della Società, di fornire ai clienti assistenza nella predisposizione di strutture che consentono di evadere gli obblighi fiscali o di trasferire risorse in violazione delle limitazioni previste dalle normative di riferimento.

Le regole di comportamento qui illustrate hanno l'obiettivo di evitare situazioni che potrebbero esporre la Società ed i suoi dipendenti ad un potenziale rischio regolamentare e legale.

I dipendenti non devono in nessun modo, direttamente o indirettamente, incoraggiare, aiutare o favorire attivamente i clienti ad eludere i principi previsti dalle normative CRS e FACTA. Tale divieto include qualsiasi atteggiamento volto a dare indicazioni, consigli e/o assistenza ai clienti al fine di definire strategie utili ad eludere gli obblighi previsti dalle normative sopra citate.

Nel caso in cui i dipendenti venissero a conoscenza di qualsiasi atto posto in essere dal cliente finalizzato al mancato rispetto degli obblighi CRS e FACTA, devono immediatamente informare l'Unità Compliance.

Da ultimo, si evidenzia che per quanto concerne l'eventuale concorso da parte della Società nella commissione del reato di sottrazione del patrimonio del cliente al pagamento delle imposte ex art. 11 del D.Lgs. 74/2000, la Società non svolge attualmente alcuna attività di consulenza sul patrimonio del cliente e non vi è quindi alcun rischio inerente a tale attività.

Rischi "indiretti"

Le attività "sensibili" identificate dal Modello nelle quali sono maggiori i rischi "indiretti" di commissione di reati tributari sono l'acquisto di beni e servizi (ciclo passivo), la contabilità e bilancio, i rapporti infragruppo, la gestione fiscale degli eventi promozionali, delle sponsorizzazioni e donazioni (compresi i rapporti con ONLUS del gruppo). Nell'ambito di tali attività potrebbero invero annidarsi in linea di principio comportamenti suscettibili di dare indirettamente luogo alla commissione di reati tributari, prevalentemente dichiarativi, da parte della Società.

Per ognuna di queste attività "sensibili" la Società ha adottato procedure interne che garantiscono un ampio sistema di controlli, con compiti specifici e differenziati. In alcuni casi, oltre alle citate procedure, la presente Parte Speciale introduce alcuni protocolli aggiuntivi, quali presidi ulteriori ritenuti utili all'esito del Risk Assessment.

Di seguito, per ciascuna delle suddette attività, si richiamano le principali procedure di riferimento, a cui si rinvia per una analisi completa e dettagliata.

Per quanto concerne l'acquisto di beni e servizi (ciclo passivo), la procedura interna di riferimento è denominata "Ciclo passivo" e prevede un articolato processo di selezione dei fornitori nell'ambito del

quale (i) il Line Manager identifica ed analizza la necessità di provvedere all'acquisto di un bene o un servizio, valuta i potenziali fornitori ed individua il fornitore più adatto per l'acquisto del bene o del servizio; (ii) la richiesta di acquisto è successivamente comunicata dal Line Manager al Direttore Finanza e Controllo, al quale spetta l'autorizzazione della richiesta dopo averne verificato il rispetto del budget assegnato all'unità organizzativa; (iii) a seguito dell'approvazione da parte del Direttore Finanza e Controllo, il Line Manager, in coordinamento con l'Unità Affari Legali e Societari, avvia l'iter per la stipula del contratto; (iv) l'Unità Affari Legali e Societari partecipa all'attività di predisposizione e di valutazione dei contratti con i fornitori e fornisce assistenza in materia legale e regolamentare. Nella sottoscrizione di contratti e documenti con i fornitori che comportano una spesa per la Società, vige il principio della doppia firma secondo il quale le persone autorizzate a rappresentare la Società possono firmare i documenti/contratti solo congiuntamente ad almeno un'altra persona avente diritto di firma, come descritto nella policy "Utilizzo della firma sociale". La procedura "Ciclo passivo" descrive poi in modo analitico le modalità di gestione, contabilizzazione e pagamento delle fatture pervenute dai fornitori della Società, che sono finalizzate a garantire il rispetto della normativa di riferimento.

Oltre ai citati presidi, la Società, quali ulteriori protocolli applicabili alla gestione del ciclo passivo, prevede che:

- prima del pagamento della fattura, la funzione che ha richiesto l'acquisto deve sempre verificare la corrispondenza quantitativa e qualitativa della prestazione ricevuta con il contratto/l'ordine d'acquisto. L'Unità Contabilità e Segnalazioni, per poter disporre il pagamento, deve dunque preventivamente ricevere l'esito positivo di tale verifica da parte della funzione richiedente.
- È inoltre previsto uno specifico processo di qualifica e selezione dei fornitori di beni e servizi, regolato da specifica Policy con la previsione degli standard qualitativi richiesti dalla Società comprensivi dei c.d. indicatori di rischio di frode carosello, l'istituzione dell'Albo fornitori, la previsione di un monitoraggio periodico sul mantenimento degli standard di qualifica, la previsione dell'obbligo di regolare il rapporto con contratto/ordine scritto che preveda le c.d. clausole 231, l'adozione del c.d. Codice Etico fornitori.

Per quanto concerne l'attività di contabilità e bilancio, la relativa procedura denominata "Contabilità e bilancio" è finalizzata alla rilevazione strutturata delle modalità, tempi e caratteristiche delle procedure da porre in essere nei processi di tenuta della contabilità generale e predisposizione del

bilancio della Società, la cui responsabilità è in capo al responsabile dell'Unità Finanza. Con specifico riferimento al processo di predisposizione del bilancio di esercizio, esso è diretto dall'Unità Finanza che fornisce tutte le informazioni ed i dettagli di contabilità al consulente fiscale esterno, affinché predisponga la bozza di calcolo delle imposte correnti ed anticipate/differite. L'Unità Finanza riceve la bozza di cui sopra e provvede alla verifica di correttezza e completezza dei dati e dei calcoli ivi riportati, inclusa una verifica di corretta interpretazione da parte del consulente fiscale delle varie voci di conto economico, per il loro corretto trattamento ai fini della determinazione delle variazioni in aumento o in diminuzione o della loro inclusione nell'ambito della base imponibile ai fini del calcolo delle imposte. Una volta completato tale iter, l'Unità Finanza provvede alla predisposizione del bilancio di verifica, dei prospetti di raccordo con il bilancio e dei prospetti di bilancio. Questi documenti sono verificati in ultima istanza dal Direttore Finanza e Controllo. Tutto il materiale predisposto viene precedentemente rivisto da e discusso con la Società di Revisione, che riporta osservazioni o riscontri in modo da poter apportare eventuali modifiche, integrazioni o correzioni alla bozza di bilancio. Nell'ambito del processo sopra descritto, tutte le attività svolte vengono dapprima ricontrollate dalla persona che le ha materialmente eseguite e, successivamente, riviste dal Direttore Finanza e Controllo, che svolge gli opportuni controlli sulle attività di contabilità generale e sugli adempimenti ad essa connessi, in modo da evitare errori e il rischio di sanzioni di carattere amministrativo e/o penale. A questi si aggiungono anche i controlli svolti da e con l'Unità Analisi di Gestione in base alle risultanze di quest'ultima. Ad ulteriore conforto delle verifiche di correttezza e completezza svolte al fine di predisporre il bilancio d'esercizio, si aggiunge un ulteriore livello di verifiche che vengono svolte dalla Società di Revisione per il rilascio della relazione di certificazione del bilancio, a cui la Società è assoggettata per obbligo normativo.

Oltre ai sopra citati protocolli, si applicano altresì i protocolli previsti nella Parte Speciale dedicata ai Reati societari. In aggiunta, infine, la Società, quale ulteriore presidio riferito ai rischi reato di natura fiscale, ha previsto meccanismi di attestazione circa la veridicità, completezza e coerenza dei dati e delle informazioni trasmesse da parte dei responsabili delle funzioni aziendali competenti della Società.

Per quanto concerne i rapporti infragruppo, si applica la policy "Prezzi di trasferimento per transazioni infragruppo", ove sono stabilite le prassi e le regole per la determinazione dei corrispettivi delle transazioni tra società del gruppo, per la predisposizione della documentazione a supporto, per l'archiviazione, per le verifiche sui prezzi di trasferimento, così come le responsabilità e le procedure

di controllo. Inoltre, in relazione all'attività di fatturazione connessa ai rapporti infragruppo, si applicano i presidi previsti dalla Procedura "Contabilità e bilancio", nella sezione "Ciclo attivo – clienti".

Per quanto concerne la gestione fiscale degli eventi promozionali, delle sponsorizzazioni e donazioni (compresi i rapporti con ONLUS del gruppo), le misure di riferimento sono contenute nella policy "Gift & Entartainment Policy", che prevede regole stringenti, inter alia, per le donazioni di beneficienza. Oltre alla citata policy, a Società ha adottato i seguenti presidi:

- è predeterminata una voce all'interno del budget annuale a cura del Direttore Finanza e Controllo destinata all'attività di sponsorizzazione, omaggistica e liberalità;
- è previsto un criterio di turnazione dei soggetti beneficiari;
- nel documentare l'attività di omaggistica e/o di sponsorizzazione, sono sempre indicate a cura del proponente le ragioni in base alle quali è stato individuato il destinatario, la tipologia di evento o regalo e il suo valore;
- il valore dell'omaggio e delle iniziative di liberalità e sponsorizzazione rispetta, oltre che il budget annuo, le linee guida adottate dall'Amministratore Delegato, che definiscono la tipologia e il valore ammessi;
- le sponsorizzazioni sono sempre regolate con contratto scritto;
- il regime fiscale applicabile alla liberalità è regolato sulla base delle previsioni contenute nella procedura denominata "Gestione adempimenti fiscali";
- le operazioni di donazione, liberalità e sponsorizzazione, sulla base della richiesta formulata dalla funzione proponente, sono sempre autorizzate dall'Amministratore Delegato; eventuali iniziative proposte dall'Amministratore Delegato sono autorizzate dal Consiglio di Amministrazione;
- è sempre prevista, a cura del Direttore Finanza e Controllo, la verifica dell'effettiva erogazione della liberalità, secondo le previsioni contrattuali e l'autorizzazione dell'Amministratore Delegato/del Consiglio di Amministrazione;
- con riferimento alla scelta del fornitore dell'omaggio o dell'evento sponsorizzato, si applicano i sopra citati protocolli previsti in relazione al "ciclo passivo", a cui si rinvia.

Per quanto concerne la gestione del personale e, in particolare, i rischi fiscali connessi alle dichiarazioni 770 e alla gestione delle note spese, la Società ha adottato le procedure denominate "Gestione adempimenti fiscali" e "Contabilità e bilancio" ("Sezione 2.6.8 - modello 770" e "Sezione 2.6.7 – note spese dipendenti e amministratori"), a cui si rinvia.

Per quanto riguarda la gestione delle risorse finanziarie e della tesoreria, la Società ha adottato procedure “Contabilità e bilancio” e “Gestione dell’attivo patrimoniale”, a cui si rinvia.