

GRADIENTE SGR S.p.A.

Modello di Organizzazione,
gestione e controllo
ex D.Lgs. 231/01

Data inizio validità: dicembre 2025

PARTE SPECIALE

A. PRINCIPI GENERALI

Obiettivo della presente Parte Speciale è la definizione di regole di condotta che indichino i comportamenti che i Destinatari del Modello devono tenere nel momento in cui operano nell'interesse o a vantaggio di Gradiente SGR S.p.A., affinché siano prevenuti comportamenti idonei a realizzare le fattispecie dei reati richiamati dal D.lgs. 231/2001.

A tal fine la Parte Speciale:

- (i) richiama le cosiddette attività "sensibili", vale a dire le attività nello svolgimento delle quali è teoricamente possibile la commissione del Reato Presupposto;
- (ii) indica i principi generali di comportamento che devono indirizzare l'attività dei Destinatari del Modello che operano nell'ambito delle suddette attività sensibili;
- (iii) indica i principi specifici di comportamento che la Società e tutti i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello.

Il Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001, nelle sue parti Generale e Speciale, si inserisce nel più ampio Sistema di Controlli sviluppato dalla Società e come tale si integra con le vigenti procedure aziendali.

I Destinatari sono tenuti a segnalare immediatamente all'OdV comportamenti rilevanti o violazioni del Modello e, se del caso, a proporre integrazioni o modifiche nei protocolli o nelle descrizioni delle aree a rischio.

Per la redazione della presente PARTE SPECIALE sono pertanto considerate rilevanti le seguenti fattispecie di reato:

- **Reati contro la Pubblica Amministrazione o l'Unione Europea** (art. 24 e 25);
- **Reato di criminalità informatica** (art. 24 bis);
- **Reati societari** (art. 25 ter);
- **Reati di criminalità organizzata** (art. 25 ter);
- **Reati con finalità di terrorismo e eversione** (art. 25 quater);
- **Reati e illeciti amministrativi di abuso di mercato;**
- **Reati in materia di salute e sicurezza sul lavoro** (art. 25 septies);
- **Reati in materia di strumenti di pagamento diversi dai contanti**
- **Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (art. 25 octies);
- **Reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;**
- **Reati ambientali** (art. 25 undicies);
- **Reati di impiego di cittadini terzi con soggiorno irregolare** (art. 25 duodecies);
- **Reati tributari** (art. 25 quinquiesdecies)

Per un maggior dettaglio degli esiti dell'attività di Risk Assessment e di cosa la Società ha introdotto per mitigare tali rischi, si rimanda all'Allegato 1 della presente Parte Speciale che contiene il documento di "Risk Assessment 231 Mappatura delle attività sensibili".

Mentre, per l'analisi approfondita delle singole fattispecie di reato richiamate dal Decreto si rinvia all'Allegato 2 "Reati 231", in cui sono riportate le informazioni inerenti alle fattispecie.

B. INDIVIDUAZIONE DELLE ATTIVITÀ SVOLTE DALLA SGR POTENZIALMENTE ESPOSTE ALLA COMMISSIONE DEI REATI PREVISTI DAL DECRETO

B.1 Il processo di identificazione delle Attività sensibili

Il Decreto, all'articolo 6 (Soggetti in posizione apicale e modelli di organizzazione dell'ente), dispone che *"Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova, fra l'altro, 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"*. In particolare, il comma 2 dell'articolo 6 indica le caratteristiche essenziali per la costruzione del Modello di organizzazione, gestione e controllo. Ai fini dell'esenzione delle responsabilità, il MOG deve quindi rispondere alle seguenti esigenze:

- a) individuare le attività nel cui ambito possono essere commessi reati;
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire.

Come si legge nella Relazione ministeriale al Decreto *"Di fatto ...All'ente viene in pratica richiesta l'adozione di modelli comportamentali specificamente calibrati sul rischio reato, e cioè volti ad impedire, attraverso la fissazione di regole di condotta, la commissione di determinati reati. Requisito indispensabile perché dall'adozione del modello derivi l'esenzione da responsabilità dell'ente è che esso venga anche efficacemente attuato: l'effettività rappresenta, dunque, un punto qualificante ed irrinunciabile del nuovo sistema di responsabilità"*.

Sebbene con l'utilizzo di una terminologia ed esposizione estranea alla pratica aziendale, le citate disposizioni si riferiscono espressamente alla costruzione di un tipico sistema di controllo interno (il Modello) secondo il classico approccio (*best practice*) seguito dagli stessi soggetti responsabili delle diverse funzioni di controllo della SGR (*Compliance, Risk management, Antiriciclaggio, Internal audit*) volto alla valutazione dei fattori di rischio e alla definizione di un appropriato piano annuale di verifica.

È del tutto evidente che vi sia quindi coincidenza "di veduta" in termini di obiettivi tra l'Organismo di Vigilanza ex 231/2001 e le altre funzioni aziendali di controllo.

Infatti, rientra nei compiti attribuiti all'OdV:

- la vigilanza sull'effettività del Modello, che si sostanzia nella verifica della coerenza tra i comportamenti concreti ed il Modello istituito;
- la disamina in merito all'adeguatezza del Modello, ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;

- l'analisi circa il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello;
- la cura del necessario aggiornamento in senso dinamico del Modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni e adeguamenti. Tale compito, di norma, si realizza in due momenti distinti ed integrati:
 - a) presentazione di proposte di adeguamento del modello al Consiglio di amministrazione;
 - b) follow-up, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

Coerentemente, quindi, con le previsioni normative l'identificazione delle aree sensibili nel MOG è stata preceduta da una serie di attività propedeutiche e preparatorie suddivise in diverse fasi e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del Decreto ed ispirate, oltre che alle norme in esso contenute, anche ai principi e suggerimenti dettati al riguardo dal Codice di Autodisciplina Assogestioni.

In particolare, sono state seguite le seguenti fasi:

- a) esame delle informazioni contenute nella relazione sulla struttura organizzativa trasmessa alle Autorità di vigilanza di settore (Consob e Banca d'Italia);
- b) esame delle procedure organizzative interne;
- c) rilevazione dei processi e delle attività svolte dalla SGR;
- d) esame degli esiti delle attività svolte dalle funzioni di controllo interno per l'individuazione dei fattori di rischio;
- e) esame dei reati previsti dal Decreto;
- f) individuazione delle Attività sensibili;
- g) *cross reference* tra ciascuna Attività sensibile e i reati previsti dal Decreto;
- h) definizione del piano controlli e dei flussi informativi verso l'OdV.

In particolare, quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni della Società, anche in relazione ai reati da prevenire, sono stati individuati:

- i principi contenuti nello Statuto Sociale;
- il Codice interno di Autodisciplina;
- le relazioni degli Amministratori al bilancio della SGR e al rendiconto dei fondi gestiti;
- il sistema disciplinare sanzionatorio previsto dal CCNL;
- il Codice di Autodisciplina Assogestioni;

- il Protocollo di autonomia dell'AIFI;
- Le *policy* e le procedure interne già adottate dalla SGR;
- le disposizioni normative e regolamentari di settore.

C. ANALISI RISCHIO REATO E MAPPATURA AREE SENSIBILI

L'analisi del rischio di reato è un'attività che ha in primo luogo l'obiettivo di individuare e contestualizzare il rischio di reato in relazione alla governance, all'assetto organizzativo e all'attività dell'ente.

In secondo luogo, attraverso tale attività si possono ottenere informazioni utili a supportare le scelte dell'OdV e del Consiglio di Amministrazione (per le rispettive competenze) in merito alle azioni di adeguamento e miglioramento del modello di organizzazione, gestione e controllo dell'ente rispetto alle finalità preventive indicate dal D. Lgs. 231/2001 (quali i livelli di esposizione ai singoli rischi di reato).

L'analisi del rischio di reato (*risk assessment 231/01*) è stata condotta tramite la valutazione dei seguenti fattori:

- l'identificazione dei rischi di reato (attraverso l'individuazione delle aree e delle attività a rischio di reato);
- la reale probabilità che un evento illecito accada (attraverso la valutazione della probabilità delle minacce che inducono o possono indurre l'evento illecito);
- il possibile danno derivante dalla realizzazione di un fatto di reato (tramite la valutazione degli Impatti);
- le debolezze aziendali di natura organizzativa che possono essere sfruttate per commettere reati (livello di Vulnerabilità).

Al fine dell'individuazione delle "aree" e delle "attività" "a rischio reato", assume preliminare rilievo la determinazione dell'ambito d'applicazione dei presupposti soggettivi del Decreto. In particolare, sono stati individuati i soggetti dalla cui condotta illecita può derivare l'estensione della responsabilità a carico della Società.

Più in dettaglio (come disposto dall'Art. 5 del D. Lgs. 231/2001):

a) da persone 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 persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Al fine di condurre il *risk assessment 231/01* GRADIENTE ha posto in essere le seguenti attività:

- I. analisi delle attività di ciascuna area aziendale, mediante interviste ai responsabili/*owners* dei processi, individuazione e mappatura delle aree «a rischio reato» e delle attività «sensibili» e «strumentali»;
- II. analisi del profilo di rischio, per ciascuna attività «sensibile» e «strumentale», mediante individuazione dei reati potenzialmente realizzabili;
- III. identificazione dei processi aziendali di riferimento nell'ambito dei quali devono essere previsti (maggiori) controlli a presidio dei rischi individuati.

Attraverso l'esame della documentazione aziendale ed una serie di interviste agli operatori «chiave» risultanti dall'organigramma della SGR, sono stati mappati i processi e analizzate le attività di ciascuna area aziendale (**censimento dei processi aziendali**) al fine di individuare le attività sensibili ove può astrattamente essere presente il rischio di commissione di alcuni dei reati del D.lgs. n.231/2001 (**mappatura dei rischi lordi**). Dopo aver valutato la qualità del controllo/presidio già attivato dalla Società viene definito il grado di rischio al netto dei presidi volti a mitigarlo (**stima dei rischi netti**).

In particolare:

A ciascuna attività sensibile è stata associata una specifica tipologia di rischio ed è stato quantificato il cosiddetto **«rischio lordo»** ovvero il rischio a cui la SGR è esposta supponendo che la stessa non abbia attivato alcun controllo e/o presidio volti a mitigarne la probabilità e l'impatto.

I rischi lordi, associati a ciascun processo, sono stati classificati in **Alti, Medi e Bassi**, sulla base di una valutazione del combinato disposto tra un punteggio di probabilità e un punteggio di impatto.

			Impatto			Rischio Lordo
			1	2	3	
Probabilità/Frequenza	1	Remota	Trascurabile	Accettabile	Critico	BASSO
	2	Poco Frequente	Trascurabile	Accettabile	Critico	MEDIO
	3	Frequente	Trascurabile	Accettabile	Critico	ALTO
	4	Molto Frequente	Trascurabile	Accettabile	Critico	

Il **«rischio netto»** è il rischio che residua dopo aver valutato la qualità del controllo/presidio già attivato dalla SGR mediante l'assegnazione di un punteggio, derivante dalla combinazione di tre tipologie di mitigazione:

- la tipologia di controllo (valutazione oggettiva), articolata in: Controlli automatici bloccanti, Controlli maker & checker, Controlli autorizzativi/gerarchici, Prassi operativa non formalizzata;
- l'efficacia dei controlli, articolata in: Adeguato, Parzialmente adeguato, Inadeguato;
- l'esistenza procedure/regolamenti, articolata in: Si adeguata, Si parzialmente adeguata, No.

Nel dettaglio, una volta assegnato a ciascuna fattispecie di rischio il relativo punteggio di «qualità dei controlli», la combinazione tra questo e il livello di «rischio lordo» determina la rilevanza del suo «rischio netto».



Sulla base degli esiti dell'attività finalizzata a individuare e valutare i rischi di reato sono stati identificati nella presente Parte Speciale specifici protocolli necessari per l'abbattimento del rischio di reato ad una misura accettabile.

D. REGOLE GENERALI DI COMPORTAMENTO

La mappatura delle aree Attività a rischio di reato ha consentito di definire i processi sensibili, nelle cui fasi, sotto fasi o attività si potrebbero in linea di principio verificare le condizioni, le circostanze o i mezzi per la commissione di Reati, anche in via strumentale alla concreta realizzazione della fattispecie di Reato.

Con riferimento a tali processi il Consiglio di Amministrazione ritiene assolutamente necessario e prioritario che nello svolgimento di attività operative siano rispettati i Protocolli indicati nella presente Parte Speciale, in quanto ritenuti idonei a prevenire i Reati tramite:

- la separazione dei compiti operativi attraverso una corretta distribuzione delle responsabilità e la previsione di più livelli autorizzativi e di controllo, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
 - la chiara e formalizzata assegnazione di responsabilità e poteri, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa;
 - la formalizzazione di regole deontologiche e comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale e dei soggetti tutelati dalle norme penali dei Reati presupposto;
 - la "proceduralizzazione" delle Attività a rischio di reato, al fine di:
 - definire e regolamentare le modalità e tempistiche di svolgimento delle attività medesime;
 - garantire la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali che attestino le caratteristiche e le motivazioni dell'operazione ed individuino i soggetti a vario titolo coinvolti nell'operazione (autorizzazione, effettuazione, registrazione, verifica dell'operazione);
 - garantire, ove necessario, l'"oggettivazione" dei processi decisionali e limitare decisioni aziendali basate su scelte soggettive non legate a predefiniti criteri oggettivo;
 - l'istituzione, esecuzione e documentazione di attività di controllo e vigilanza sulle Attività a rischio di reato;
 - l'esistenza di meccanismi di sicurezza che garantiscano un'adeguata protezione delle informazioni dall'accesso fisico o logico ai dati e agli asset del sistema informativo aziendale, in particolare con riferimento ai sistemi gestionali e contabili.
- In linea generale:
- La SGR ha definito un proprio Sistema Organizzativo che prevede i seguenti presidi di controllo:
- l'emanazione di deleghe di funzioni e disposizioni organizzative avviene direttamente dal Consiglio di Amministrazione e/o dall'Amministratore Delegato;

- l'organigramma è formalizzato a tutti i livelli aziendali e da questo emergono con chiarezza e trasparenza le funzioni, i ruoli e le linee di riporto;
- il periodico aggiornamento da parte dell'Alta Direzione e la formalizzazione a tutti i livelli aziendali ogni qualvolta ci siano mutamenti sostanziali nell'organizzazione tali da richiederne la diffusione;
- la formalizzazione a tutto il personale aziendale, sulla base delle deleghe di funzioni e disposizioni organizzative emanate, delle mansioni e delle responsabilità di ciascuna struttura organizzativa;
- la predisposizione di mansionari, policy e procedure attraverso il confronto diretto con i responsabili delle diverse aree organizzative;
- la diffusione e informazione circa l'organizzazione in essere attraverso strumenti condivisi e accessibili da parte dei dipendenti, finalizzati a garantire la chiarezza organizzativa (cartelle di rete condivise);
- la predisposizione di report sull'esercizio delle deleghe per l'organo che ha conferito delega/procura.

Più in particolare il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei reati (rintracciabilità ed evidenza delle operazioni sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative e per "procura" il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

Ai titolari di una funzione aziendale (generalmente dirigenti non facenti parte del consiglio di amministrazione) che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza viene conferita una "procura generale funzionale" di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la "delega".

I requisiti essenziali del sistema di deleghe, ai fini di un'efficace prevenzione dei reati sono i seguenti:

- la formazione e l'attuazione delle decisioni della Società rispondano ai principi ed alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del presente Modello e delle procedure aziendali;
- le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma, devono essere rese note all'interno della Società e comunicati all'Organismo di Vigilanza anche qualora debbano essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna delega deve definire in modo specifico ed inequivoco:
 - i poteri del delegato.
 - Il soggetto (organo o individuo) cui il delegato riporta gerarchicamente.
 - I poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali.
- Il delegato deve disporre di poteri di spesa adeguati alle funzioni conferite. Ogni operazione e/o transazione aziendale deve essere autorizzata nel rispetto delle deleghe, coerente, documentata, registrata ed in ogni momento verificabile;

- non vi sia identità soggettiva tra coloro che decidono e pongono in essere una “operazione sensibile” e coloro che risultano investiti del potere di destinarvi le necessarie risorse economiche e finanziarie;
- è garantita la separazione dei compiti, attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
- esistenza e documentazione di attività di controllo e supervisione, compiute sulle decisioni e transazioni aziendali.

I protocolli/presidi di carattere specifico riportati di seguito per ciascuna fattispecie di reato richiamano il rispetto totale dei principi di carattere generale.

Di seguito, per ciascuna fattispecie di reato si riportano:

- l'elenco dei reati ricompresi nell'ambito della fattispecie;
- le aree sensibili della SGR a rischio reato;
- i principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo;
- le procedure specifiche adottate dalla SGR per ciascuna area sensibile.

E. PARTI SPECIALI

1. REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI

1.1 Le fattispecie di reato nei confronti della Pubblica Amministrazione

Le fattispecie di reato nei confronti della Pubblica Amministrazione o dell'Unione Europea, contemplate agli artt. 24, 24 bis e 25 del D. Lgs. 231/01, comprendono:

Art. 24 – Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico o frode nelle pubbliche forniture.

- **Malversazione di erogazioni pubbliche (Art. 316-bis c.p.)** – Presupposto del reato in esame è l'avvenuta erogazione da parte di un ente pubblico o dalla UE in favore di un soggetto attivo di una somma per la realizzazione di opere di interesse pubblico. Ai sensi dell'art. 316 bis c.p. risponde a tale reato chiunque, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato o dall'UE, da un altro ente pubblico contributi, sovvenzioni o finanziamenti per la realizzazione di opere o per lo svolgimento di attività di pubblico interesse, non li destina a dette attività
- **Indebita percezione di erogazioni pubbliche a danno dello Stato (Art. 316-ter c.p.)** – Presupposto del reato è che l'erogazione pubblica sia conseguita a mezzo dell'esibizione di documentazione falsa ovvero per l'omissione di informazioni dovute. La Società sarà chiamata a

rispondere in sede penale ove la condotta illecita sia stata posta in essere dai suoi funzionari, in tal modo assicurando all'istituto un finanziamento al quale non avrebbe diritto

- **Truffa a danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640 c.p.)** – Tale ipotesi di reato si realizza qualora un dipendente o rappresentante della SGR, attraverso artifici o raggiri (es, esibendo documenti falsi), induca lo Stato o un ente pubblico in errore, ricavandone un profitto cagionando un danno allo Stato o all'ente pubblico
- **Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640-bis c.p.)** – Presupposto del reato è che la truffa riguardi l'erogazione di contributi, sovvenzioni, finanziamenti, mutui agevolati ed altre erogazioni concesse da parte dello Stato, di enti pubblici o della Comunità Europea. Si rinvia a quanto osservato nei casi previsti agli artt. 316-ter e 640 del c.p.. Si pensi ad esempio a truffe perpetuate ai danni di enti previdenziali, ovvero amministrazioni locali o ripartizioni di queste, attraverso dichiarazioni mendaci o altre condotte fraudolente.
- **Frode informatica se commessa in danno dello Stato o di altro ente pubblico (Art. 640-ter c.p.)** – Tale ipotesi di reato si configura nel caso di alterazione del funzionamento di un sistema informatico o telematico o di intervento senza diritto su dati, informazioni, programmi allo scopo di trarne profitto con danno d'altri. Ad esempio, è configurabile nel caso in cui, attraverso l'alterazione del software di controllo INPS per le denunce retributive, si ottenga un ingiusto vantaggio con danno dell'Ente previdenziale.
- **Frode nelle pubbliche forniture (art. 356 c.p.)** - Commette il reato chiunque nell'esecuzione di contratti di fornitura con lo Stato, con un altro ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità non adempia ai propri obblighi, facendo ricorso ad artifici o raggiri tali da ingannare la controparte sul contenuto della propria prestazione, facendo mancare in tutto o in parte cose o opere necessarie a uno stabilimento pubblico o a un servizio pubblico. La pena è aumentata se la fornitura concerne sostanze alimentari o medicinali, ovvero cose od opere destinate alle comunicazioni, all'armamento o equipaggiamento delle forze armate, o ad ovviare a un comune pericolo o a un pubblico infortunio.
- **Frode ai danni del Fondo europeo agricolo (art. 2 L. n. 898/1986)** - Tale disposizione punisce chiunque mediante l'esposizione di dati o notizie falsi ottiene per sé o per altri aiuti, premi, indennità, restituzioni o erogazioni in genere a carico, anche solo in parte, al Fondo europeo agricolo di garanzia o al Fondo europeo agricolo per lo sviluppo rurale. A tali erogazioni sono assimilate le quote nazionali complementari rispetto a quelle erogate dai predetti Fondi nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa UE in materia. Modello di organizzazione, gestione e controllo – versione 2 Semestre 2020 56 Quando la condotta non consista nella sola falsità delle informazioni, ma sia caratterizzata da artifici o raggiri di effettiva portata decettiva ricorre il più grave reato di truffa ai danni dello Stato.

Art. 25 – Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione. (Articolo modificato dalla L. n. 190/2012, dalla L. n. 3/2019, dal D.Lgs. n. 75/2020, dalla L. 112/2024 e dalla L. 114/2024)

- **Peculato (art. 314, comma 1, e art. 316 c.p.)** - Il reato è commesso dal pubblico ufficiale o dall'incaricato di pubblico servizio che si appropria di denaro o di beni mobili altrui di cui abbia per

ragione di servizio il possesso o la disponibilità, oppure che riceve o trattiene indebitamente per sé o per terzi denaro o altra utilità, percepiti approfittando dell'errore altrui. Tali condotte comportano la responsabilità amministrativa ai sensi del D. Lgs. n. 231/2001 solo se i fatti offendano gli interessi finanziari dell'UE. Si tratta di illeciti contestabili in situazioni in cui non ricorrano gli elementi di altri reati, quali ad esempio quello di truffa ai danni dell'UE.

- **Concussione (art. 317 c.p.)** – Commette tale reato il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando delle sue qualità o dei suoi poteri, costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità.
- **Corruzione per l'esercizio della funzione (art. 318 c.p.) – Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o dipendente della SGR dia o prometta a un Pubblico Ufficiale, per sé o per altri, denaro o altra utilità (es. doni in natura) per omettere o ritardare, per avere omesso o ritardato, un atto del suo ufficio, ovvero per compiere o per avere compiuto un atto contrario ai doveri di ufficio. Il reato si configura sia nei confronti del corrotto che del corruttore.
- **Corruzione in atti giudiziari (art. 319 ter c.p.)** – Si caratterizza rispetto ai reati precedenti sotto il profilo del dolo specifico. Tale ipotesi di reato si verifica qualora il dipendente o rappresentante della SGR corrompa un magistrato o un testimone al fine di ottenere favori in un procedimento civile, penale o amministrativo che vede coinvolta la stessa società o un soggetto terzo.
- **Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)** - Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità. Il reato si configura nei confronti anche dell'indotto.
- **Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)** – Tale ipotesi di reato si configura nel caso in cui la corruzione per un atto d'ufficio o per un atto contrario ai doveri di ufficio riguardino un Incaricato di Pubblico Servizio.
- **Istigazione alla corruzione (art. 322 c.p.)** - Tale ipotesi di reato si configura nel caso in cui il dipendente o rappresentante della SGR offra denaro o altra utilità a un Pubblico Ufficiale o ad un Incaricato di Pubblico Servizio per una finalità corruttiva ma l'offerta o la promessa non sia accettata.
- **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte Penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui un dipendente o rappresentante della SGR commetta i delitti di peculato, concussione, induzione indebita a dare o promettere utilità e istigazione alla corruzione con riguardo ai membri delle istituzioni comunitarie (Commissione Europea, Parlamento Europeo, Corte di Giustizia, Corte dei Conti).

- **Traffico di influenze illecite (art. 346 bis c.p.)** – Tale ipotesi di reato si configura allorquando chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

1.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione dei rapporti con le Autorità di Vigilanza;**
- **Gestione dei rapporti con Enti pubblici;**
- **Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze;**
- **Stipula e gestione dei rapporti contrattuali con clienti e controparti;**
- **Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi;**
- **Gestione dei contenziosi.**
- **Gestione di sponsorizzazioni, donazioni, eventi, manifestazioni e omaggistica.**

In relazione all'operatività della SGR, a titolo esemplificativo e non esaustivo, si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione i seguenti:

- Amministrazioni dello Stato, anche a ordinamento autonomo, Comuni, Regioni e Province;
- I Ministeri, i Dipartimenti e le Commissioni;
- Aziende municipalizzate e gli Enti pubblici trasformati in S.p.A. (ad es.: Poste Italiane, FS, ecc.);
- Camere di commercio, industria, artigianato, agricoltura e l'Ufficio del Registro;
- Gli enti pubblici economici e gli enti pubblici non economici nazionali, regionali e locali (INPS, ENASARCO, INAIL, ISTAT);
- Le amministrazioni, le aziende e gli enti del Servizio Sanitario regionale;
- Banca d'Italia, Consob, Agenzia delle Entrate, Guardia di Finanza, Autorità Garante della Privacy, etc.

Per le finalità previste dal presente documento, si considerano non solo i rapporti "diretti", ma anche quelli "indiretti" con soggetti che - notoriamente - intrattengono rapporti di qualsivoglia natura (parentela, affinità, coniugio, convivenza, ecc.) con Pubblici Ufficiali o Incaricati di Pubblico Servizio.

1.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 1.1.

All'uopo, è fatto **divieto** in particolare di:

- compiere azioni o tenere comportamenti che siano o possano essere interpretati come pratiche di corruzione, favori illegittimi, comportamenti collusivi, sollecitazioni, dirette o mediante terzi, di privilegi per sé o per altri rilevanti ai fini della commissione dei reati di cui al Decreto;
- adottare comportamenti contrari alle Leggi, al Codice Interno di Comportamento e, più in generale, alle Procedure aziendali, in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o quando questi siano controparte del contenzioso, al fine di influenzarne le decisioni nell'interesse della SGR;
- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità di Vigilanza in errore;
- chiedere o indurre i rappresentanti dell'Autorità di Vigilanza a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l'esercizio delle funzioni di Vigilanza;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dai presidi aziendali o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti dell'Autorità di Vigilanza a titolo personale con la finalità di promuovere o favorire interessi della SGR;
- concludere contratti di consulenza con soggetti interni alla Pubblica Amministrazione o all'Unione Europea in base ai quali si potrebbe minare l'imparzialità e il buon andamento della Pubblica Amministrazione o dell'Unione Europea stessa;
- chiedere o indurre i soggetti della Pubblica Amministrazione o dell'Unione Europea a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di stipulare accordi/convenzioni/contratti con la SGR;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti della Pubblica Amministrazione o dell'Unione Europea a titolo personale con la finalità di promuovere o favorire interessi della SGR. Tra i vantaggi che potrebbero essere accordati, si cita, a titolo esemplificativo ancorché non esaustivo, la promessa di assunzione per parenti ed affini.
- alterare il funzionamento di un sistema informatico o telematico ovvero di intervenire senza diritto sui dati, informazioni o programmi contenuti nel sistema di scambio di dati con le Autorità di Vigilanza;

- effettuare o promettere, in favore dei clienti, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito onde evitare di costituire fondi utilizzabili per la commissione di uno dei reati;
- assegnare incarichi di fornitura ed incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della SGR che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi onde evitare di costituire fondi utilizzabili per la commissione di uno dei reati;
- riconoscere, in favore dei Consulenti compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente nel settore di attività interessato;
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Interno di Comportamento e dalle procedure operative aziendali; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione o all'Unione Europea e alla conseguente possibilità di agevolare l'instaurazione/sviluppo di rapporti finalizzati alla stipula;

Ai fini dell'attuazione dei divieti suddetti, dovranno rispettarsi le **regole generali** di seguito indicate:

- i rapporti con la Pubblica Amministrazione o l'Unione Europea devono avvenire nell'assoluto rispetto delle leggi, delle normative vigenti, dei principi di lealtà e correttezza, nonché dei principi contenuti nel Modello 231;
- tutti coloro che materialmente intrattengono rapporti con la P.A. o con l'Unione Europea devono essere in possesso di apposita autorizzazione da parte della SGR;
- la gestione delle attività svolte nell'ambito delle Aree/Processi a Rischio dovrà avvenire esclusivamente ad opera delle funzioni/soggetti aziendali competenti;
- le attività svolte nell'ambito delle Aree/Processi a Rischio devono essere disciplinate in modo da dettagliare ogni fase del processo, evidenziare le attività svolte, i controlli/le verifiche eseguiti e il processo autorizzativo; identificare in maniera chiara i soggetti e le funzioni che svolgono le varie attività (attività operative-gestionali, attività di controllo, attività di autorizzazione/approvazione); definire le modalità e la responsabilità per la documentazione e la tracciabilità delle singole attività svolte;

- il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione o dell'Unione Europea; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
- il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni;
- tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
- è necessario mantenere una segregazione dei compiti tra i differenti soggetti coinvolti nei vari processi sensibili finalizzati ad intrattenere rapporti con gli Enti Pubblici, in particolare:
 - con riferimento alla gestione dei rapporti non riconducibili alla ordinaria operatività delle Unità Organizzative della SGR, tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività aziendale indirizzata alle Autorità di Vigilanza è sottoposta all'attenzione della Funzioni Compliance;
 - le attività di cui alle diverse fasi dei Processi a Rischio devono essere svolte da soggetti differenti chiaramente identificabili;
- i processi sia a livello informativo sia in termini documentali devono essere tracciabili, in particolare:
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Unità Organizzativa è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione o l'Unione Europea;
 - completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutte le Unità Organizzative interessate, di una reportistica sulle erogazioni effettuate/contratti stipulati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione o dell'Unione Europea di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso;
- i soggetti e le funzioni coinvolte nelle Aree/Processi a Rischio devono osservare scrupolosamente le indicazioni contenute nelle specifiche a disciplina delle attività svolte nei processi stessi;
- tutti coloro che materialmente intrattengono rapporti con la Pubblica Amministrazione o l'Unione Europea per conto GRADIENTE (ivi inclusi i rapporti intrattenuti in occasione di effettuazione di verifiche ispettive o sopralluoghi) devono godere di un'autorizzazione in tal senso da parte della SGR stessa, consistente in un'apposita delega o direttive organizzative interne per i dipendenti, i e gli organi sociali ovvero in un contratto di fornitura/consulenza o di collaborazione opportunamente formalizzato;

- i Destinatari non possono effettuare o promettere, in favore dei terzi, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi instaurato o che non siano debitamente formalizzate in un contratto o in un accordo, ad es. con la finalità di influenzare il giudizio del pubblico funzionario nel caso di verifiche ispettive;
- in particolare, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. Le procedure aziendali illustrano i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
- la SGR può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che promuovono i principi etici conformi a quelli della SGR;
- per quanto attiene gli omaggi e le spese di rappresentanza destinati, seppure in modo non esclusivo, ad esponenti della Pubblica Amministrazione o dell'Unione Europea, le Direttive e Procedure aziendali stabiliscono idonei limiti quantitativi rapportati al valore di tali omaggi/spese;
- per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa;
- i responsabili delle funzioni della SGR coinvolti nelle Aree a Rischio devono garantire il costante aggiornamento e sensibilizzazione del personale e dei terzi coinvolti Aree a Rischio circa i contenuti del Modello e sulla normativa di riferimento per lo svolgimento della attività con soggetti appartenenti alla Pubblica Amministrazione o dell'Unione Europea;
- eventuali situazioni di incertezza in ordine ai comportamenti da tenere (anche in ragione dell'eventuale condotta illecita o semplicemente scorretta del Pubblico Ufficiale), all'interpretazione della normativa vigente e delle procedure interne devono essere sottoposte all'attenzione del superiore gerarchico e/o dell'OdV;
- l'OdV dovrà essere inoltre informato per iscritto di qualsivoglia elemento di criticità/irregolarità dovesse insorgere nell'ambito del rapporto con la Pubblica Amministrazione o l'Unione Europea.

1.4 Procedure Specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate dalla SGR.

1.4.1 Gestione dei rapporti con autorità di Vigilanza e altri organismi pubblici ispettivi

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione dei rapporti con le Autorità di Vigilanza in occasione di adempimenti, comunicazioni, anche attraverso l'utilizzo della PEC, e visite ispettive, previsti dalla normativa di riferimento.

Fra le Autorità di Vigilanza con cui la SGR può trovarsi a intrattenere rapporti si indicano, a titolo esemplificativo:

- Banca d'Italia;
- Consob;
- Unità di Informazione Finanziaria (U.I.F.);
- Autorità Garante per la Privacy;
- Camera di Commercio;
- Guardia di Finanza.

Ai sensi del D.lgs. n. 231/2001, le attività in oggetto potrebbero presentare potenzialmente occasioni per la commissione dei reati di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, corruzione verso la Pubblica Amministrazione (nelle sue diverse fattispecie), induzione indebita a dare o promettere utilità.

Dall'analisi critica delle procedure in essere è emerso che le attività più specificamente a rischio di commissione dei reati nella gestione dei rapporti con le Autorità di Vigilanza sono le seguenti:

- **Gestione degli accessi e dei rapporti in caso di visite ispettive (es. Consob, Banca d'Italia,);**
- **Adempimenti in materia di Vigilanza Informativa e Statistica;**
- **Gestione Atti giudiziari, accertamenti Guardia di Finanza.**

Sulla base del sistema dei poteri e delle deleghe della SGR i rapporti con le Autorità di Vigilanza sono gestiti dall'Amministratore Delegato.

In particolare, l'Amministratore Delegato, per i poteri ad esso conferiti, rappresenta la Società, nei confronti degli enti previdenziali (INPS), nei confronti delle Autorità di vigilanza nonché nei confronti di qualunque altra Autorità o ufficio pubblico e privato in Italia.

Sulla base delle procedure operative della SGR, gli uffici competenti: i) affiancano l'Amministratore Delegato nei rapporti con le Autorità di Vigilanza; ii) collaborano nel fornire le informazioni necessarie ad alimentare il flusso delle segnalazioni afferenti la SGR e i FIA gestiti; iii) collaborano nella redazione delle risposte alle richieste di dati, informazioni o notizie pervenute dalle Autorità di Vigilanza; iv) provvedono a formulare ed inviare richieste e quesiti alle Autorità di Vigilanza; v) curano rapporti con gli Organi di Vigilanza durante lo svolgimento della procedura di approvazione/modifiche del Regolamento di Gestione e del Prospetto d'offerta dei FIA gestiti dalla SGR.

L'Amministratore Delegato ha facoltà di sostituire a sé dipendenti della Società solo mediante il rilascio delle deleghe necessarie e dandone successiva comunicazione al Consiglio.

Gli atti che impegnano la SGR nei confronti dell'Autorità di Vigilanza devono essere sottoscritti soltanto dai soggetti incaricati.

Nell'ambito di visite ispettive effettuate da parte delle Autorità presso la sede della SGR:

- i rapporti con le autorità di vigilanza e con altri organismi pubblici ispettivi sono intrattenuti dall'Amministratore Delegato o da altri soggetti di riferimento appositamente incaricati tramite delega interna da conservare a cura dell'Ufficio Amministrazione e Finanza;
- in caso di visita ispettiva il Responsabile della struttura/funzione interessata dall'ispezione mantiene adeguata evidenza di tutte le fasi di raccolta ed elaborazione delle informazioni richieste e trasmesse, degli sviluppi dell'indagine e del suo esito;
- la Funzione Compliance e la Funzione AML devono essere tempestivamente informate della visita ispettiva, dei suoi sviluppi e del suo esito;

- ad ogni visita ispettiva da parte di Funzionari rappresentanti delle Autorità di Vigilanza, il Responsabile della funzione/struttura interessata provvede a trasmettere all'Amministratore Delegato gli eventuali verbali rilasciati dal Funzionario pubblico e degli annessi allegati;
- In caso di ispezione da parte dell'Autorità di Vigilanza, è prescritta in ogni caso la massima collaborazione da parte di tutte le strutture/funzioni aziendali interessate dall'ispezione

La SGR ha affidato in outsourcing - mediante appositi contratti disciplinanti il livello dei servizi prestati - l'attività di amministrazione contabile della SGR e dei FIA gestiti, compresi gli adempimenti di vigilanza informativa e statistica nei confronti delle Autorità di Vigilanza.

L'outsourcer amministrativo, sulla base degli impegni assunti nel contratto (corredato da appositi SLA) assicura la corretta e completa predisposizione dei contenuti delle comunicazioni e il loro puntuale invio secondo le modalità e i tempi previsti dalla richiesta dell'Autorità;

L'outsourcer amministrativo adotta modalità di controlli automatici in relazione alle attività di segnalazione aventi caratteristiche di periodicità;

I processi di controllo delle attività poste in essere dall'*Outsourcer* amministrativo fanno capo all'Ufficio Amministrazione e Finanza, con l'ausilio della Funzione Compliance.

E' previsto, in capo a tutte le strutture/funzioni della SGR, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni ed adempimenti alle Autorità di Vigilanza, l'obbligo di archiviazione e conservazione della documentazione prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico.

1.4.2 Gestione dei rapporti con gli Enti pubblici (INPS, INAIL, Ag. Entrate ecc.)

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione dei rapporti con gli Enti Pubblici in occasione di adempimenti, comunicazioni, anche attraverso l'utilizzo della PEC, previsti dalla normativa di riferimento, nonché di attività legate alla gestione dei FIA della SGR.

Fra gli Enti pubblici con cui la SGR può trovarsi a intrattenere rapporti si indicano, a titolo esemplificativo:

- Inps;
- Inail;
- Inpdap;
- Direzione Provinciale del Lavoro;
- Medicina del Lavoro;
- Agenzia delle Entrate;
- Camera di Commercio;
- Enti pubblici Locali.

Ai sensi del D.lgs. n. 231/2001, le attività in oggetto potrebbero presentare potenzialmente occasioni per la commissione dei reati di Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, Corruzione verso la Pubblica Amministrazione (nelle sue diverse fattispecie), Induzione indebita a dare o promettere utilità.

Dall'analisi critica delle procedure in essere è emerso che le attività più specificamente a rischio di commissione dei reati nella gestione dei rapporti con gli Enti pubblici sono le seguenti:

- **Gestione dei rapporti con gli Enti pubblici per assolvere gli obblighi derivati dalla gestione del personale e per dare esecuzione agli adempimenti fiscali della SGR.**

Sulla base del sistema e delle deleghe della SGR l'Amministratore Delegato ha facoltà di sostituire a sé dipendenti della Società solo mediante il rilascio delle deleghe necessarie e dandone successiva comunicazione al Consiglio.

Gli atti che impegnano la SGR nei confronti degli Enti Pubblici devono essere sottoscritti soltanto dai soggetti incaricati.

Per gli adempimenti di legge relativi alla gestione del personale la SGR si avvale di un consulente del lavoro.

Il consulente del lavoro, sulla base degli impegni assunti nel contratto assicura il corretto e completo adempimento degli obblighi di legge in materia di gestione del personale dipendente; l'attività viene monitorata costantemente dall'Ufficio Amministrazione e Finanza.

Le strutture aziendali interessate provvedono all'archiviazione di tutta la documentazione inerente l'esecuzione degli adempimenti svolti.

1.4.3 Gestione approvvigionamenti, incarichi professionali e consulenze

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze.

Dall'analisi critica delle procedure in essere è emerso che le attività più specificamente a rischio di commissione dei reati nella gestione dei rapporti con gli Enti pubblici sono le seguenti:

- **Gestione incarichi professionali e consulenze sia nei confronti della SGR che dei FIA gestiti;**
- **Esternalizzazione funzioni operative essenziali o importanti o di servizi.**

Sulla base dei poteri e delle deleghe e delle procedure aziendali i poteri di spesa relativi alla stipula di contratti di acquisto di beni e/o servizi e incarichi professionali sono chiaramente attribuiti, in funzione della natura della spesa e dei limiti di importo definiti nell'ambito del sistema di deleghe e poteri vigente e del relativo budget assegnato.

Le modalità di selezione e pagamento dei fornitori di beni e servizi e dei professionisti esterni sono disciplinate da apposite procedure aziendali, è effettuata sulla base di un iter approvativo da parte delle competenti strutture/funzioni aziendali ed effettuata secondo criteri basati su parametri oggettivi e trasparenti.

La SGR detta disposizioni particolari in caso di esternalizzazione di funzioni essenziali o importanti, così come individuate dalla normativa di settore. In particolare, nella scelta del fornitore la SGR presta particolare attenzione ai criteri di i) presenza di ogni abilitazione e/o autorizzazione e/o requisito richiesti dalla disciplina di riferimento per l'esecuzione delle prestazioni; ii) professionalità e competenza riconosciuta nel mercato di riferimento; iii) costo delle prestazioni. La selezione e qualifica di fornitori particolarmente critici (esternalizzazione funzioni essenziali) è responsabilità diretta del Consiglio di Amministrazione.

Al fine di garantire la liceità e la piena pertinenza di ogni rapporto di affari che la SGR intrattiene con i propri fornitori, si richiede al fornitore/consulente/professionista una dichiarazione di presa visione del Codice Interno di Comportamento e di impegno ad attenersi ai principi e alle regole che compongono il Modello di Organizzazione, Gestione e Controllo (ex D.lgs. 231/01) con l'espresso avvertimento che a fronte di eventuali violazioni verranno adottate delle sanzioni, quali la risoluzione del contratto stesso.

Nel caso non sia possibile inserire la suddetta clausola negli accordi tra società e soggetto terzo, la SGR invia mediante posta elettronica certificata o lettera raccomandata A.R. o a mani, un'informativa finalizzata a notificare alla controparte l'esistenza di un Codice Interno di Comportamento, che fa parte di un Modello di Organizzazione, Gestione e Controllo (ex D.lgs. 231/01) adottato dalla SGR. La SGR si accerta di ricevere, come risposta all'informativa, una specifica dichiarazione di avvenuta presa di conoscenza.

Nella gestione di ogni relazione con i fornitori, i Destinatari si attengono a quanto stabilito nel Codice Interno di Comportamento e nella Policy per la gestione di potenziali situazioni di conflitto di interesse personale e interesse dell'azienda.

L'autorizzazione al pagamento della fattura spetta alla funzione competente a seguito del controllo di congruenza della prestazione/fornitura ricevuta da parte della funzione di riferimento. E' previsto un controllo sulle fatture relative ai beni/servizi richiesti propedeutici all'autorizzazione al pagamento al fine di riscontrare il rispetto dell'iter autorizzativo previsto; in particolare, al ricevimento delle fatture, l'Ufficio Amministrazione e Finanza – acquisita l'autorizzazione al pagamento dal settore competente - effettua controlli di congruità e procede alla registrazione e all'archiviazione del documento.

Il pagamento delle fatture viene normalmente effettuato tramite bonifico bancario a mezzo servizio home banking. Ogni pagamento deve essere preventivamente autorizzato dall'Amministratore Delegato.

Sono previsti controlli di coerenza delle spese sostenute rispetto al budget assegnato al Responsabile di riferimento.

La SGR adotta una specifica procedura interna finalizzata a disciplinare l'attività di monitoraggio e valutazione periodica in merito alla qualità dell'operato dei fornitori/*outsourcer* e controllo sui costi derivati dall'attività svolta

L'Ufficio Amministrazione e Finanza archivia in apposito raccoglitore, o in formato elettronico in apposita cartella di rete, il preventivo/contratto (o altra documentazione ricevuta, attestante la spesa che la Società dovrà sostenere) in attesa di ricevere la relativa fattura.

Con particolare riferimento ai rapporti con gli Enti Pubblici, viene altresì definito che:

- ciascuna fase rilevante in caso di accordi con la Pubblica Amministrazione o l'Unione Europea deve risultare da apposita documentazione scritta;
- ogni accordo/convenzione/contratto con Enti pubblici è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- deve essere garantita la documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte.

1.4.4 Stipula e gestione dei rapporti contrattuali con clienti e controparti

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla stipula e gestione dei rapporti contrattuali con la clientela.

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti altresì in attività connesse alla stipula e gestione dei rapporti contrattuali con i clienti e con altre controparti.

Dall'analisi critica delle procedure in essere è emerso che le attività più specificamente a rischio di commissione dei reati nella gestione dei rapporti con gli Enti pubblici sono le seguenti:

- Gestione dei rapporti con i sottoscrittori dei FIA gestiti**

- Gestione dei rapporti con le controparti nell'ambito del processo di investimento/disinvestimento.**

Il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla selezione e gestione dei rapporti con la clientela e con le controparti contrattuali. Ciascuna fase rilevante degli accordi con la clientela risulta da apposita documentazione scritta.

Ogni accordo/convenzione/contratto con i clienti è formalizzato in documenti scritti, ai sensi della normativa vigente, debitamente firmati da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere, e opportunamente archiviati.

Nell'ambito della gestione dei FIA, la SGR adotta procedure che definiscono per le operazioni di investimento/disinvestimento specifici presidi di controlli e livelli autorizzativi per l'identificazione e la gestione delle controparti; al Consiglio di Amministrazione viene attribuito il potere di approvare i processi di investimento e ne verifica periodicamente l'adeguatezza.

In materia di incentivi, il Consiglio di Amministrazione verifica periodicamente l'efficacia dei presidi organizzativi assicurando che il sistema dei flussi informativi sia adeguato, completo e tempestivo.

L'Amministratore Delegato, con il supporto della struttura, attua le misure organizzative e le procedure per la gestione degli incentivi definite dal Consiglio di Amministrazione e ne cura costantemente l'adeguatezza. Specifiche attività di controllo sono attribuite alla Funzione Compliance.

1.4.5 Gestione del processo di selezione e assunzione del personale e del sistema degli incentivi

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione del processo di selezione e assunzione del personale e del sistema di corresponsione degli incentivi.

La SGR adotta un'apposita procedura per la selezione e assunzione del personale con modalità e iter autorizzativi differenziati per dirigenti e altro personale dipendente.

In particolare, la selezione del personale avviene sulla base di specifiche procedure che garantiscano una valutazione dei candidati effettuata nel rispetto dei seguenti principi: effettiva esigenza di nuove risorse; previa acquisizione del curriculum del candidato e svolgimento di colloqui attitudinali; omogeneità delle informazioni raccolte sui candidati mediante compilazione di apposita modulistica; valutazione comparativa sulla base di criteri obiettivi di professionalità, preparazione e attitudine in

relazione alle mansioni per le quali avviene l'assunzione che sono stati definiti a priori della fase di selezione; motivazione esplicita delle ragioni poste alla base della scelta.

Per la selezione e assunzione del personale Dirigente viene richiesta l'acquisizione del certificato dei carichi pendenti e casellario giudiziale.

Il processo di selezione/assunzione del personale è disciplinato in modo da dettagliare ogni fase del processo, evidenziare le attività svolte, i controlli/le verifiche eseguiti e il processo autorizzativo; identificare in maniera chiara i soggetti e le funzioni che svolgono le varie attività (attività operative-gestionali, attività di controllo, attività di autorizzazione/approvazione); definire le modalità e la responsabilità per la documentazione e la tracciabilità delle singole attività svolte.

Tutta la documentazione di supporto al processo di selezione e assunzione di ciascun dipendente viene archiviata a cura dell'Ufficio Amministrazione e Finanza.

Il Budget per l'assunzione di personale e i piani interni di sviluppo, ivi compresi i sistemi premianti e di incentivazione, viene autorizzato secondo il vigente sistema dei poteri e delle deleghe.

La SGR adotta una specifica Policy in cui vengono illustrate le politiche e le prassi di remunerazione ed incentivazione che la SGR attua in ottemperanza alla normativa vigente in materia. La policy disciplina altresì la cessazione del rapporto lavorativo e relativi pagamenti di buona uscita.

Resta inteso che è fatto in particolare divieto effettuare o promettere, in favore di pubblici funzionari italiani ed esteri o a loro parenti, anche per interposta persona, proposte di assunzione tali da influenzare il giudizio del pubblico funzionario relativo alla definizione di un accordo ovvero nel corso di un rapporto con la SGR di qualsivoglia natura, ivi comprese le situazioni in cui tali comportamenti possano condizionare il giudizio di esponenti della Pubblica Amministrazione o dell'Unione Europea nel corso di ispezioni, verifiche e/o sopralluoghi.

1.4.6 Gestione dei contenziosi

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione dei contenziosi giudiziali e stragiudiziali (amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi.

Ai sensi del D.lgs. 231/2001, le attività in oggetto potrebbero presentare potenzialmente occasioni per la commissione dei reati di Corruzione verso la Pubblica Amministrazione (nelle sue diverse fattispecie) e Corruzione in atti giudiziari, Induzione indebita a dare o promettere utilità, Truffa ai danni dello Stato, Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria, Corruzione tra privati.

È fatto espresso divieto di:

- indurre Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio) a favorire indebitamente gli interessi della SGR e/o influenzarne il giudizio/parere;
- indurre all'indebito superamento di vincoli o criticità ai fini della tutela degli interessi della SGR;
- favorire indebitamente gli interessi della SGR inducendo, con violenza o minaccia o, alternativamente, con offerta o promessa di denaro o di altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;

- influenzare le posizioni della Pubblica Amministrazione quando questa sia controparte del contenzioso/arbitrato.
- affidare incarichi a professionisti legali esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa;
- riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili.

Il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla facoltà di comporre in via transattiva eventuali controversie, prevedendo adeguati livelli quantitativi oltre ai quali le singole transazioni devono essere autorizzate dal Consiglio di Amministrazione e fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

Il sistema dei poteri e delle deleghe definisce le facoltà di autonomia per la gestione del contenzioso, precisando i soggetti autorizzati e i limiti per la promozione di azioni giudiziarie; disciplina il sistema di attribuzione delle procure alle liti sia nelle cause attive che in quelle passive, anche in relazione a procedimenti di natura monitoria e d'urgenza.

Le procedure aziendali prevedono e disciplinano il conferimento degli incarichi a legali esterni.

1.4.7 Gestione di sponsorizzazioni, donazioni, eventi, manifestazioni e omaggistica

La SGR può effettuare erogazioni sotto forma di donazioni o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi della legge e che non contrastino con i principi etici della SGR.

I Destinatari si attengono a quanto disposto dal Codice Interno di Comportamento e dalle procedure aziendali in materia di sponsorizzazioni, donazioni, eventi, manifestazioni e omaggistica

In ogni caso è fatto divieto di:

- effettuare, per conto della società, erogazioni, per iniziative di donazione o di sponsorizzazione, a favore di Enti coinvolti in note vicende giudiziarie, pratiche non rispettose dei diritti umani o dell'ambiente;
- effettuare elargizioni/omaggi a favore di Enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel precedente paragrafo ovvero nella normativa interna;
- promettere o concedere vantaggi di qualsiasi natura – direttamente o indirettamente - a rappresentanti della Pubblica Amministrazione / delle Autorità di Vigilanza o altre organizzazioni/persone collegate - anche su induzione degli stessi - ovvero a esponenti apicali o a persone a loro subordinate di società private con finalità di promuovere o favorire interessi della SGR, anche a seguito di illecite pressioni.
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con la SGR, al fine di favorire indebitamente gli interessi della SGR;

- dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere nonché le indicazioni geografiche e le denominazioni di origine protette.

Inoltre, il Personale deve immediatamente segnalare al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza.

1.5 Controlli dell'Organismo di Vigilanza

Con riferimento alle attività a rischio, l'Organismo di Vigilanza ha facoltà discrezionale di:

- verificare che i rapporti con la Pubblica Amministrazione o l'Unione Europea siano in linea con i principi sanciti nel Codice Interno di Comportamento e con le procedure aziendali;
- verificare che i rapporti con esponenti della Pubblica Amministrazione o dell'Unione Europea siano intrattenuti soltanto da dipendenti appositamente autorizzati;
- verificare il rispetto della segregazione funzionale nel processo di invio di dati e comunicazioni ad Aziende ed Enti Pubblici ed alle Autorità di Vigilanza;
- verificare che nel corso di ispezioni e verifiche da parte di pubblici funzionari, i soggetti autorizzati abbiano prestato un adeguato livello di collaborazione e fornito tempestivamente le informazioni ed i documenti richiesti;
- accertare che il contenzioso giudiziale ed extra giudiziale sia gestito nel rispetto della normativa vigente e delle deleghe e procure;
- verificare il rispetto della segregazione funzionale nel processo di pagamento a favore di Aziende ed Enti Pubblici;
- verificare la corretta applicazione delle procedure in tema di selezione del personale, dei fornitori, sponsorizzazioni, donazioni ed uscite di cassa.

2. REATI DI CRIMINALITÀ INFORMATICA

2.1 Le fattispecie di reati di delitti informatici e trattamento illecito di dati

I reati presupposto contenuti nella presente Parte Speciale sono disciplinati dall'articolo 24 – bis del Decreto, come da ultimo modificato dal Decreto-legge 21 settembre 2019, n. 105, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

- **Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR falsifichi un documento informatico pubblico o privato, avente efficacia probatoria. A tal fine, per "documento informatico" si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, con esclusione dunque dei programmi informatici. Ad esempio, un dirigente della SGR ruba la smart card necessaria per utilizzare la firma digitale "forte" di un amministratore delegato di un'azienda concorrente, al fine di modificare un documento informatico avente valore legale, laddove per firma digitale "forte" si intende la firma elettronica la cui

provenienza e integrità è stata preventivamente certificata da un Ente certificatore legalmente autorizzato.

- **Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. A tal fine, per “sistema informatico” si intende qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l’esecuzione di un programma per elaboratore, compiono l’elaborazione automatica di dati (si è ritenuto, ad es., che anche un semplice personal computer possa essere considerato un vero e proprio sistema, per la ricchezza dei dati contenuti). Ad esempio, un dipendente della società accede, anche indirettamente tramite un apposito programma (“spyware”), al computer di un’azienda concorrente al fine di visualizzare i termini dell’offerta che quest’ultima intende presentare ad una gara d’appalto alla quale anche la società intende partecipare.
- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR abusivamente si procuri, riproduca, diffonda, comunichi o consegna codici o parole chiave o altri mezzi idonei all’accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo, al fine di procurare a sé o ad altri un profitto o di recare un danno ad altri. Ad esempio, un dipendente della SGR si procura un codice d’accesso (password, smart card, ecc.) idoneo ad introdursi da remoto nella rete aziendale di una società concorrente. Il Decreto Legge 13/2022 ha modificato l’articolo 615-quater c.p. che ora vede una nuova rubricazione, un ampliamento delle condotte punibili e una modificazione in termini di cornice edittale. La nuova disposizione, rubricata ora “Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all’accesso a sistemi informatici o telematici”, prevede che sia punibile il soggetto che “abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti idonei all’accesso ad un sistema informatico o telematico protetto da misure di sicurezza al fine di arrecare a sé o ad altri un profitto o di arrecare ad altri un danno”. La pena della reclusione si estende sino a due anni nell’ipotesi base, mentre da uno a tre anni se ricorre una delle circostanze di cui all’articolo 617- quater comma 4.
- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR si procuri, diffonda, comunichi o consegna un programma informatico avente per scopo o per effetto di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l’interruzione (totale o parziale) o l’alterazione del suo funzionamento. Ad esempio, un dipendente della SGR diffonde, all’interno del sistema informatico appartenente all’azienda concorrente, un programma virus contenuto in un supporto rimovibile (chiave USB, CD, DVD), o tramite posta elettronica, che diffondendosi e riproducendosi mina la funzionalità di detto sistema.

A seguito del Decreto Legge 13/2022, l’articolo 615-quinquies c.p. è ora rubricato “Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a

danneggiare o interrompere un sistema informatico o telematico" e così come modificato dalla suddetta legge, si connota per una nuova formulazione della condotta punibile ora rivolta a "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR intercetti fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa. Il reato si configura altresì qualora si riveli, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle predette comunicazioni. Ad esempio, un dipendente della SGR invii continuamente messaggi di posta elettronica (spam) ad un'azienda concorrente al fine di rallentare o bloccare le loro reti e i loro servizi di posta elettronica.

A seguito del Decreto Legge 13/2022, all'art. 617-quater c.p., vengono inasprite le pene per l'ipotesi di cui al primo comma ora punita con la reclusione "da un anno e sei mesi a cinque anni", nonché di quella prevista dal comma quarto per la quale si prevede un innalzamento della pena edittale "da tre a otto anni". L'articolo 617-quinquies ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche" si connota per una nuova formulazione relativa alle condotte punibili che prevedono ora l'attivazione della risposta sanzionatoria nei confronti di chiunque "procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi" con il fine di "intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle".

- **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR installi apparecchiature atte ad intercettare, impedire, o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Ad esempio, un dipendente della SGR installa in alcuni terminali aziendali di un competitor un software ("trojan horse" o "spyware") che contiene una scheda che consente di intercettare informazioni riservate utili per la SGR.
- **Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR distrugga, deteriori, cancelli, alteri o renda inservibili, anche parzialmente, informazioni, dati o programmi informatici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante. Ad esempio, la SGR assolda un *hacker* (o *cracker*) che modifica il sito web dell'azienda concorrente (cosiddetto "*web defacing*"), facendo apparire informazioni false o tali da compromettere la reputazione dell'azienda stessa.

- **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.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR distrugga, deteriori, cancelli o renda inservibili informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.
- **Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR distrugga, danneggi, deteriori, o renda inservibili, anche parzialmente, sistemi informatici o telematici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante. Ad esempio, un dipendente della SGR trasmette una e-mail contenente virus ai sistemi informatici appartenenti ad un'azienda concorrente, provocando un malfunzionamento dei sistemi informatici utilizzati dalla stessa azienda, paralizzandone l'attività lavorativa.
- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della SGR distrugga, danneggi, deteriori, renda inservibili, anche parzialmente, i sistemi informatici o telematici di pubblica utilità, ovvero ne ostacoli il corretto funzionamento. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante. Ad esempio, GRADIENTE inserisce dei virus nei sistemi informatici appartenenti alla società fornitrice di energia elettrica, provocando un malfunzionamento del sistema di rendicontazione dei Kw consumati da GRADIENTE stessa.
- **Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui il soggetto che presta servizi di certificazione di firma elettronica violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri un danno. Trattandosi di un reato proprio, lo stesso sarà configurabile per GRADIENTE qualora la condotta venga posta in essere in concorso con il soggetto "che presta servizi di certificazione delle firme elettroniche". Ad esempio, un dipendente di GRADIENTE corrompe un certificatore al fine di ottenere un certificato in realtà appartenente ad una persona fittizia.
- **Ostacolo alle procedure in tema di definizione, gestione e controllo del "Perimetro di sicurezza nazionale cibernetica" (art. 1, comma 11 D.L. n. 105/2019)** - Il reato punisce chi, allo scopo di ostacolare o condizionare le Autorità preposte a tutelare il sistema delle infrastrutture tecnologiche strategiche:
 - 1) fornisce informazioni, dati o elementi di fatto non rispondenti al vero rilevanti:
 - a) per la predisposizione e aggiornamento degli elenchi delle reti, dei sistemi (comprensivi della relativa architettura e componentistica) e dei servizi informatici della PA e degli operatori pubblici e privati con sede in Italia, dai quali dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di servizio essenziale per le attività civili, sociali o economiche fondamentali e dal cui malfunzionamento, interruzione o abuso possa derivare un pericolo per la sicurezza nazionale;
 - b) ai fini delle comunicazioni che detti operatori pubblici e privati devono effettuare al CVCN (Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello Sviluppo

economico) dei contratti di fornitura che intendano stipulare per approvvigionarsi di beni, sistemi e servizi ICT destinati a essere impiegati nelle reti, sistemi e servizi di cui al punto che precede;

c) per lo svolgimento delle attività ispettive e di vigilanza concernenti il rispetto delle disposizioni e procedure inerenti alla predisposizione e aggiornamento dei predetti elenchi, alla comunicazione delle forniture e alla notifica degli incidenti e alle misure di sicurezza relative ai sopra menzionati, sistemi, reti e servizi;

2) omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

La persona fisica che commette un reato di criminalità informatica è punita con la reclusione da un minimo di sei mesi ad un massimo di otto anni e con una multa fino a 10.329 Euro.

Per la Società sono previste sanzioni pecuniarie da 100 a 500 quote (da 25,8 mila Euro a 774,5 mila Euro) e sanzioni interdittive ex art. 9, comma 2 del D.Lgs. 231/2001, per un periodo da tre mesi a due anni.

2.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione e utilizzo dei sistemi informativi della SGR.**

Come descritto nella Parte Generale al Capitolo 4 dedicato alla descrizione dell'approccio metodologico adottato per l'aggiornamento del Modello, con specifico riferimento alle analisi e valutazioni condotte in materia di criminalità informatica, per sua natura tema pervasivo di diversi ambiti ed attività aziendale, l'attenzione è stata posta su quello che può essere definito quale il processo di "gestione della sicurezza informatica".

Il rischio di potenziale commissione dei reati in oggetto è per la natura stessa di tali fattispecie delittuose, potenzialmente "presente" in tutte le attività svolte dai dipendenti o da collaboratori a progetto/lavoratori interinali/somministrati della SGR che prevedono l'utilizzo dei sistemi e degli applicativi informatici (IT) di Gradiente.

In considerazione di quanto sopra esposto, possono essere ritenuti coinvolti nella gestione della sicurezza tutti i dipendenti, collaboratori a progetto, lavoratori interinali/somministrati ecc. a prescindere dalla loro collocazione, dalla forma della loro collaborazione con la società, dalle mansioni svolte e dal livello gerarchico, in quanto sono obbligati a svolgere le loro attività nel rispetto del sistema delle regole e norme di riferimento per l'utilizzo dell'IT.

Tuttavia, il rischio potenziale, in termini di probabilità di accadimento di uno dei reati in materia informatica e relative conseguenze, può essere valutato in correlazione alle caratteristiche delle attività svolte e ai sistemi IT utilizzati. In conseguenza di ciò, anche il sistema dei controlli adottato per mitigare il livello di rischio identificato presenta un livello di articolazione coerente con la natura e il livello potenziale del rischio specifico.

Le aree ritenute essere esposte ad un maggior rischio possono essere riconducibili a quelle a cui sono delegate compiti inerenti alcuni processi per la gestione della sicurezza informatica (autorizzazione accessi ai sistemi) e quelle in cui la frequenza, la complessità e la criticità nell'utilizzo dell'IT è maggiore e in cui le competenze informatiche dei soggetti coinvolti risultano più elevate.

2.3 Principi di controllo e di comportamento e di assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 2.1.

Il Personale è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (ad esempio, personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività professionale. Tali risorse devono essere conservate in modo appropriato e la SGR deve essere tempestivamente informata di eventuali furti o danneggiamenti.

Il Personale è tenuto alla segnalazione alle competenti strutture di eventuali incidenti di sicurezza, anche concernenti attacchi al sistema informatico da parte di hacker esterni).

E' in particolare fatto divieto di:

- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della SGR o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, trojan, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato contemplate nel Decreto, nonché atti idonei diretti in modo non equivoco a realizzarle;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato, possano potenzialmente diventarlo.

2.4 Procedure Specifiche

2.4.1 Gestione della sicurezza dei sistemi informatici e dei dati

Il server adottato dalla SGR e tutti i servizi collegati dispongono di credenziali di accesso univoche per utente o operatore, standardizzate alle normative attuali e rilasciate unitamente ad un documento informativo che attesta l'area di validità delle stesse e al regolamento aziendale che disciplina l'utilizzo dei sistemi informativi.

L'operatività degli utenti è infine tracciata secondo quanto previsto dalla normativa vigente, nel rispetto della normativa sulla privacy e disciplinari collegati.

La gestione e manutenzione delle apparecchiature informatiche utilizzate dalla SGR è affidata ad un outsourcer, sulla base di uno specifico contratto di fornitura di servizi.

L'Ufficio Amministrazione e Finanza intrattiene i rapporti con l'outsourcer informatico per la risoluzione delle eventuali problematiche emerse nell'utilizzo dei sistemi *software* e *hardware* necessari al mantenimento in efficienza della SGR.

Il backup delle informazioni avviene automaticamente su un dispositivo NAS dedicato ed agisce a livello di partizione logica, senza entrare nel merito del contenuto della stessa. Le procedure di backup sono eseguite ad intervalli regolari e prevedono il salvataggio di snapshot, tali informazioni sono accessibili solo con l'utenza amministrativa della NAS.

Per quanto riguarda l'infrastruttura di rete, la SGR utilizza una connessione internet, protetta da firewall dedicato. Il firewall ruota il traffico da e verso Internet utilizzando un indirizzo IP Pubblico univoco e tale indirizzo è indicato quale indirizzo unico nei pubblici registri dei servizi internet, quali il database Whois e simili. La configurazione del firewall permette di utilizzare i servizi erogati dal server anche da remoto, attraverso un canale criptato secondo la tipologia del servizio, che può essere identificato come certificato digitale SSL o rete privata virtuale VPN.

Tutte le postazioni di lavoro client, sia di tipo notebook sia di tipo desktop, sono attestate al dominio logico del server sopra descritto, implementando il servizio di single sign-on alle procedure e servizi aziendali. Ricevono automaticamente gli aggiornamenti di sicurezza relativi al software antivirus da internet tramite la piattaforma cloud Solarwinds MSP. La politica di gestione di quest'ultimo è implementata a livello centrale e non è modificabile dalle singole postazioni di lavoro.

Le procedure di Disaster Recovery prevedono il recupero delle informazioni direttamente dalla NAS di backup in quanto trattasi di immagini dell'intero ambiente logico, avviabili indipendentemente dall'hardware sottostante. Questo approccio permette di rendere l'intero ambiente versatile e facilmente riavviabile in ambienti diversi da quello nativo oggetto del disastro. Non è previsto un backup in un sito alternativo.

Il servizio antivirus è gestito in cloud tramite la piattaforma Solarwinds MSP la cui manutenzione è affidata a Project Informatica Srl Unipersonale (già Centro Computer).

Gli amministratori, i dipendenti, i collaboratori professionisti, devono attenersi ad un principio generale di diligenza e correttezza nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo della SGR. Ogni utilizzo del sistema informativo della società diverso da finalità strettamente professionali è espressamente vietato.

In attuazione delle misure di sicurezza richieste la SGR ha adottato, in apposite procedure aziendali, i presidi procedurali, organizzativi ed informatici per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine della società.

Utilizzo dell'elaboratore e della rete interna.

L'accesso all'elaboratore della propria postazione di lavoro, sia esso collegato in rete o "stand alone", è protetto da un sistema di autenticazione. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza.

Su ogni elaboratore della società è stato installato un software antivirus per prevenire eventuali danneggiamenti causati dalla presenza di virus informatici. Nonostante la presenza del software antivirus è possibile che riescano ugualmente ad installarsi nei computer virus informatici non identificati o riconoscibili. Pertanto, in caso si evidenzino avvisi, messaggi di errore o anomalie di funzionamento del computer va effettuata tempestiva segnalazione al titolare del trattamento, ai fini della relativa risoluzione.

Le unità di rete e le aree di condivisione contengono informazioni strettamente professionali e non possono essere utilizzate per scopi diversi.

Stampanti e fax in aree sono collocate in ambienti accessibili a soggetti non abilitati al trattamento e non presidiati.

Utilizzo servizi vari su internet

I servizi on line devono essere esclusivamente finalizzati al reperimento di informazioni utili all'attività della SGR.

E', pertanto, vietato ogni utilizzo dell'accesso su internet, non finalizzato allo svolgimento della propria attività lavorativa o di tipo personale.

Al fine di non compromettere la sicurezza della SGR e di prevenire conseguenze legali o di altro genere a carico della SGR, gli utenti dovranno osservare le cautele di seguito descritte:

- evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione;
- osservare il divieto di partecipazione a forum non professionali, utilizzo di chat, di bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet non strettamente inerenti all'attività professionale.

Utilizzo del servizio di posta elettronica

Al fine di non compromettere la sicurezza della società e di prevenire conseguenze legali a carico della SGR stessa sono osservate le cautele di seguito descritte:

- se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi) tali mail non devono essere “aperte” e i predetti file devono essere eliminati tempestivamente;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando documenti non pertinenti all'esercizio dell'attività della SGR.

Gestione dei documenti cartacei

La documentazione cartacea contenente dati personali o sensibili deve essere protetta in appositi “scaffali” chiusi a chiave. Le chiavi sono conservate a cura dei soggetti che, di volta in volta, gestiscono i singoli archivi:

- Segreteria;
- Amministrazione e Finanza;
- Team di Investimento.

È vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni.

Selezione e gestione password

Al fine di garantire la massima sicurezza dei dati aziendali e la protezione da accessi indesiderati alla rete interna, per accedere al sistema ad ogni utente è assegnato un identificativo di accesso (User ID).

La password viene scelta dall'utente senza restrizioni di sorta. Il Responsabile Amministrazione, Finanza non può variare la password; può, con il supporto della società che presta assistenza informatica, intervenire soltanto nel caso in cui l'utente smarrisca o dimentichi la propria password, sostituendo quest'ultima con un'altra provvisoria che è sovrascritta a sua volta dalla password scelta dall'utente.

L'obiettivo della sicurezza è perseguito limitando agli utenti l'accesso ai menù del sistema informativo.

A ciascun utente è consentito l'accesso al proprio menù del sistema (relativo alla propria area funzionale) e non ad altri (abilitazione).

La SGR, ai sensi della vigente normativa, ha previsto un “Piano di Continuità Operativa” (c.d. Piano di Business Continuity) che definisce gli attori, le strategie ed identifica le eventuali azioni e soluzioni di continuità adottate che consentono di mantenere un livello di qualità sufficiente dei servizi erogati, anche in presenza di eventi avversi tali da minare la possibilità per la Società di continuare ad operare nelle proprie funzioni caratteristiche.

Qualora sia previsto il coinvolgimento di soggetti terzi (a titolo esemplificativo, fornitori, consulenti e professionisti) nelle attività a rischio-reato di cui alla presente Parte Speciale, il sistema dei controlli e i principi di comportamento ivi contenuti si applicano anche a presidio delle attività poste in essere dagli stessi.

2.5 Controlli dell'Organismo di Vigilanza

Con riferimento ai processi a rischio identificati nella presente sezione, l'Organismo di Vigilanza ha il compito di verificare:

- l'adozione ed il periodico aggiornamento da parte della SGR di procedure operative e regolamenti interni relativi alla sicurezza dei sistemi informatici e dei dati, opportunamente diffusi e rispettati dai dipendenti;
- il corretto funzionamento dei processi di autenticazione e di accesso ai sistemi informatici ed ai dati;
- che la Società abbia, nei termini di legge, aggiornato il Documento Programmatico sulla Sicurezza dei dati (ex D.Lgs. 196/2003);
- l'efficacia ed il rispetto delle procedure previste per la protezione delle reti;
- la corretta implementazione ed il rispetto delle procedure previste per la protezione ed il salvataggio dei dati (procedure di *backup*, *disaster recovery*);
- l'adeguatezza e la puntuale implementazione delle procedure previste per la protezione delle aree, dei locali *server* e delle postazioni di lavoro;
- il corretto svolgimento dei processi di trasmissione dei dati, informazioni e documenti all'esterno dell'azienda;
- l'osservanza della procedura relativa alla consegna di strumenti, supporti informatici e credenziali di accesso ai dipendenti.

3 REATI SOCIETARI

3.1 Le fattispecie di reati societari

L'art. 3 del D.Lgs. n. 61 dell'11 aprile del 2002, ha introdotto l'art. 25 ter¹ del D.Lgs. 231/2001, modificato dalla Legge n. 69/2015, che, per i reati previsti, prevede l'applicazione della sola sanzione pecuniaria, con l'esclusione delle sanzioni interdittive (fatte salve le fattispecie di corruzione tra privati ed istigazione alla corruzione tra privati per le quali, a seguito delle novelle legislative di cui al Decreto legislativo, 15/03/2017 n° 38, G.U. 30/03/2017, si applicano anche le sanzioni interdittive di cui all'articolo 9, comma 2 del D.Lgs. n. 231/2001).

All'interno di tale fattispecie si possono prevedere i seguenti articoli del codice civile:

- **False comunicazioni sociali (art. 2621 c.c.)** – Tale ipotesi di reato si realizza se gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci, i liquidatori della SGR, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, espongono consapevolmente nei bilanci, relazioni o altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ovvero omettono di fornire notizie la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale

¹ L'art. 25-ter è stato modificato da:

- L. n. 190/12, che ha aggiunto il riferimento al nuovo reato di "Corruzione tra privati", di cui all'art. 2635, comma 3, del codice civile, con decorrenza dal 28 novembre 2012;
- L. n. 69/15, che ha eliminato per i reati societari i riferimenti a condizioni di responsabilità degli enti in parte diverse da quelle ordinarie e ha riformato i reati di false comunicazioni sociali, con decorrenza dal 14 giugno 2015.

o finanziaria della SGR, in modo idoneo a indurre in errore i destinatari delle suddette comunicazioni.

- **Fatti di lieve entità (art. 2621-bis c.c.)** - Salvo che costituiscano più grave reato, si applica la pena 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. Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando 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.
- **False comunicazioni sociali delle società quotate (art. 2622 c.c.)** – Tale fattispecie di reato si realizza se gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni.
- **Impedito controllo (art. 2625, 2° comma c.c.)** – Tale reato si configura qualora, occultando documenti o con altri idonei artifici, gli amministratori della SGR impediscano o comunque ostacolino lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, al collegio sindacale o alla società di revisione cagionando un danno ai soci.
- **Indebita restituzione dei conferimenti (art. 2626 c.c.)** – Tale figura di reato si realizza nel caso in cui un amministratore della SGR, fuori dei casi di legittima riduzione del capitale sociale e sotto qualsiasi forma, restituisca ai soci i conferimenti o li liberi dall'obbligo di eseguirli.
- **Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)** – Tale figura di reato ricorre nel caso in cui gli amministratori della SGR ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite.
- **Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)** - Tale figura di reato si configura qualora gli amministratori della SGR acquistino o sottoscrivano, al di fuori dei casi previsti dalla legge, azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
- **Operazioni in pregiudizio dei creditori (art. 2629 c.c.)** – Tale figura di reato si realizza nel caso in cui gli amministratori della SGR violando le disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.
- **Omessa comunicazione del conflitto di interessi (Art. 2629 bis c.c.)** – L'amministratore, che in una determinata operazione ha, per conto proprio o di terzi, interesse in conflitto di interessi con quello della Società, non ne dà debita comunicazione agli altri amministratori e non si astiene dal partecipare alle deliberazioni riguardanti l'operazione stessa.

- **Corruzione tra privati (art. 2635 c.c.)**
- **Formazione fittizia del capitale (art. 2632 c.c.)** – Tale figura di reato si configura qualora gli amministratori e i soci conferenti della SGR anche in parte, formino od aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o di quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.
- **Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)** - Tale fattispecie di reato si configura nell'ipotesi in cui l'eventuale liquidatore di società, ripartendo i beni sociali prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli, cagioni danno ai creditori stessi.
- **Art. 2636 c.c. – Illecita influenza sull'assemblea** – Il reato si attua qualora con atti simulati o con frode si determini la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto. Tale reato può essere commesso da chiunque ("reato comune"), e quindi anche da soggetti esterni alla Società. La commissione di questo reato non si configura in quanto la SGR è socio unico.
- **Aggiotaggio (art 2637 c.c.)** – Tale fattispecie di reato ricorre qualora, ad esempio, il soggetto apicale di società diffonda notizie false ovvero ponga in essere operazioni simulate o altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, 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.)** – Tale fattispecie di reato si realizza qualora nelle comunicazioni alle autorità di vigilanza previste ai sensi della normativa applicabile in materia si espongano fatti materiali non corrispondenti al vero, ovvero si occultino con altri mezzi fraudolenti fatti che si sarebbero dovuti comunicare, al fine di ostacolare l'esercizio delle funzioni di vigilanza*.

La persona fisica che commette un reato societario è punita con la reclusione da un minimo sei mesi ad un massimo di otto anni e con una multa fino a 10.329 Euro.

Per la Società sono previste sanzioni pecuniarie da 100 a 1.000 quote (da 258 mila Euro a 1.549 mila Euro).

Con specifico riferimento al reato di corruzione tra privati, per la Società è prevista una sanzione pecuniaria da 400 a 600 quote. Per il reato di istigazione alla corruzione tra privati, è invece prevista una sanzione pecuniaria da 200 a 400 quote.

Per entrambe le fattispecie di reato, alla sanzione pecuniaria si sommano le sanzioni interdittive di cui all'art. 9, comma 2, del D.lgs. 231/2001.

3.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Operazioni di rilevazione, registrazione e rappresentazione delle attività della SGR e dei Fondi gestiti nelle scritture contabili, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa e di gestione degli aspetti fiscali.**
- **Gestione dei Rapporti con il Collegio Sindacale e la Società di Revisione.**

Con specifico riferimento ai reati di Corruzione tra privati, Istigazione alla corruzione tra privati e Ostacolo all'esercizio delle funzioni dell'autorità di vigilanza e Omessa comunicazione del conflitto di interessi, si rimanda alla Parte Speciale *"REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI"*, ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

3.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 3.1.

All'uopo, è fatto divieto in particolare di tenere i seguenti comportamenti/effettuare le seguenti operazioni:

- impedire od ostacolare in qualunque modo, anche occultando documenti o utilizzando altri idonei artifici, lo svolgimento delle attività istituzionali di controllo;
- determinare o influenzare illecitamente l'assunzione delle deliberazioni assembleari, ponendo a tal fine in essere atti simulati o fraudolenti che si propongano di alterare artificiosamente il normale e corretto procedimento di formazione della volontà assembleare;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione di bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della SGR;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della SGR;
- illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della SGR e sull'evoluzione della sua attività, nonché sugli eventuali strumenti finanziari e relativi diritti;
- diffondere, concorrere a diffondere, in qualunque modo, informazioni, notizie o dati falsi o porre in essere operazioni fraudolente o comunque fuorvianti in modo anche solo potenzialmente idoneo a provocare un'alterazione del prezzo di strumenti finanziari.

Ai fini dell'attuazione dei divieti suddetti, dovranno rispettarsi le regole di seguito indicate:

- i Destinatari devono: a) comportarsi sempre con diligenza, correttezza e trasparenza, nell'interesse del pubblico degli investitori e del mercato; b) organizzarsi in modo da escludere la ricorrenza di situazioni di conflitto di interesse e, in tali occasioni, assicurare comunque l'equilibrata tutela degli interessi in conflitto; c) adottare misure affinché non si realizzi un'indebita circolazione/diffusione, all'interno della SGR, di informazioni rilevanti;
- mantenere un comportamento corretto, trasparente e collaborativo al fine di garantire la tutela del risparmio degli investitori;
- porre la massima attenzione ed accuratezza in ogni attività finalizzata all'acquisizione, elaborazione ed illustrazione di dati e di informazioni relative a prodotti finanziari necessari per permettere agli investitori di formare un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della SGR;
- i rapporti con il Collegio Sindacale e la Società di Revisione sono intrattenuti dal Responsabile dell'Unità Organizzativa di riferimento o dai soggetti dal medesimo appositamente incaricati;
- i Destinatari devono osservare una condotta improntata a principi di integrità, correttezza e trasparenza nell'attività di formazione del bilancio, delle relazioni e delle altre comunicazioni sociali previste dalla legge, in modo da fornire ai soci e al pubblico informazioni veritiere e corrette sulla situazione economica, patrimoniale e finanziaria della SGR, nel rispetto di tutte le norme di legge, regolamentari e dei principi contabili applicativi;
- deve essere garantita una tempestiva e completa evasione, a cura delle strutture competenti, delle richieste di documentazione specifica avanzate dalla Società di Revisione nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili: ciascuna Unità Organizzativa ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori;
- deve essere garantita una segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Collegio Sindacale e la Società di Revisione;
- i Destinatari devono garantire il puntuale rispetto di tutte le norme di legge che tutelano l'integrità e l'effettività del capitale sociale, al fine di non creare nocumeto alle garanzie dei creditori e, più in generale, ai terzi.

3.4 Procedure Specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate dalla SGR.

3.4.1 Operazioni di rilevazione, registrazione e rappresentazione delle attività della SGR e dei Fondi gestiti nelle scritture contabili, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa e di gestione degli aspetti fiscali

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse ad operazioni di rilevazione, registrazione e rappresentazione dell'attività di impresa

nelle scritture contabili, nei bilanci, nelle relazioni sulla gestione, nei prospetti informativi e in altri documenti di impresa e di gestione degli aspetti fiscali.

Ai sensi del d.lgs. n. 231/2001, le attività in oggetto potrebbero presentare potenzialmente occasioni per la commissione dei reati di false comunicazioni sociali, false comunicazioni sociali con fatti di lieve entità e false comunicazioni sociali in danno della società, dei soci o dei creditori.

La registrazione delle scritture contabili e la redazione del bilancio di esercizio sono effettuate nel rispetto dei principi estimativi e valutativi, previsti dalla legge, da normative internazionali e da procedure interne riguardanti poste di bilancio o criteri di contabilizzazione.

Tutti i costi e oneri, ricavi e proventi, incassi e esborsi sono rappresentati in contabilità in modo veritiero e corretto, opportunamente documentati in conformità alla legislazione vigente.

Per la redazione del bilancio, la Società applica i principi contabili internazionali (IAS e IFRS) emanati dall'International Accounting Standard Board e le relative interpretazioni dell'International *Financial Reporting Interpretation Committee* (IFRIC).

La SGR adotta procedure contabili interne, costantemente aggiornate, in cui sono indicati con chiarezza: i) i dati e le notizie da fornire; ii) i criteri contabili per l'elaborazione dei dati; iii) la tempistica della trasmissione dei dati.

Per la predisposizione del bilancio annuale e delle situazioni contabili semestrali, il Settore Amministrazione della SGR si avvale del supporto dell'outsourcer amministrativo.

I contratti con gli outsourcer amministrativi disciplinano gli obblighi in capo all'outsourcer e definiscono standard di servizio; le procedure operative del Settore Amministrazione prevedono, per ciascuna fase operativa eseguita dall'outsourcer, specifiche attività di controllo e di spunta dei dati registrati in contabilità;

In particolare, sono attivati specifici controlli interni finalizzati a verificare:

- con cadenza periodica, i saldi di contabilità generale;
- i saldi dei conti lavorazione, transitori e similari;
- la produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
- l'analisi degli scostamenti, attraverso il confronto dei dati esposti nel periodo corrente e quelli relativi a periodi precedenti;
- la quadratura della versione definitiva del bilancio con i dati contabili.

Le dichiarazioni fiscali vengono visionate e verificate dal Responsabile del Settore Amministrazione e Finanza con il supporto del consulente fiscale;

La rilevazione delle informazioni contabili avviene per il tramite di sistemi e applicativi informatici, a garanzia della tracciabilità di ogni singola fase del processo di definizione dei dati.

Il progetto di bilancio è approvato di norma dal Consiglio di Amministrazione per poi essere portato all'attenzione dell'assemblea degli azionisti.

I documenti di gestione dei fondi gestiti sono approvati dal Consiglio di Amministrazione.

La SGR predispone il budget aziendale che viene elaborato dall'Amministratore Delegato, con il supporto del Responsabile Settore Amministrazione e Finanza e sottoposto all'approvazione del Consiglio di Amministrazione.

La revisione dei bilanci della SGR è affidata ad una Società di Revisione in conformità alle disposizioni normative vigenti.

3.4.2 Gestione dei rapporti con il Collegio Sindacale e la Società di Revisione

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione dei rapporti con il Collegio Sindacale e i Soci, nell'ambito delle attività di controllo attribuite agli stessi, e con la Società di revisione, nell'ambito delle proprie attività di revisione e certificazione del bilancio.

Ai sensi del D.lgs. n. 231/2001, le attività in oggetto potrebbero presentare potenzialmente occasioni per la commissione dei reati di Impedito controllo e Corruzione tra privati.

Il Settore Amministrazione, con il supporto dell'outsourcer amministrativo, presta collaborazione alla Società di Revisione e al Collegio Sindacale per lo svolgimento delle attività di controllo sulle registrazioni contabili e sul bilancio della SGR.

I criteri di selezione, valutazione e di conferimento dell'incarico alla Società di revisione sono formalizzati, fermo il disposto dell'art. 160 T.U.F.

E' prevista la sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo posti in essere dal Collegio Sindacale e/o dalla Società di revisione.

Le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal Collegio Sindacale o dalla Società di revisione, sono documentate e conservate dalla SGR.

3.5 Controlli dell'Organismo di Vigilanza

Con riferimento alle attività a rischio, l'Organismo di Vigilanza ha il compito di:

- verificare periodicamente il rispetto delle Procedure Amministrative e Contabili e l'esito dei controlli periodici;
- verificare periodicamente l'effettuazione delle comunicazioni alle Autorità di Vigilanza e l'osservanza delle procedure adottate nel corso di eventuali controlli;
- verificare che la società di revisione sia selezionata nel rispetto della procedura ed eventuali ulteriori incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, non siano conferiti alla società di revisione, ovvero siano espressamente adottati specifici presidi nel caso in cui vengano attribuiti incarichi di due diligence a società del gruppo di appartenenza della società di revisione attestanti l'assenza di correlazioni.
- controllare che le richieste inoltrate dagli organi di controllo siano tempestivamente recepite e evase;

- verificare che i rapporti con i Clienti siano in linea con i principi sanciti, nel Codice Interno di Comportamento e con le procedure aziendali;
- verificare la corretta applicazione delle procedure a disciplina dei Processi a rischio richiamati nella presente Parte Speciale.

4 REATI IN MATERIA DI CRIMINALITA' ORGANIZZATA

4.1 La fattispecie di reato in materia di criminalità organizzata

L'art. 2, comma 29, della Legge n. 94 del 15 luglio 2009, "Disposizioni in materia di sicurezza pubblica", ha introdotto l'art. 24 ter del D.Lgs. n. 231/2001 "Delitti di criminalità organizzata"

che richiama i seguenti articoli del codice penale:

- **Associazione per delinquere finalizzata (416 c.p.)** – Associazione realizzata da tre o più persone finalizzata:
 - alla riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
 - alla tratta di persone (art. 601 c.p.);
 - all'acquisto e alienazione di schiavi (art. 602 c.p.);
 - ai reati concernenti le violazioni delle disposizioni in materia di immigrazione clandestina (art. 12 d. lgs. 286/1998);
- **Associazione per delinquere di stampo mafioso anche straniera (416 bis c.p.)** – Associazione di tipo mafioso formata da tre o più persone. L'associazione è di tipo mafioso 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, di appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasioni di consultazioni elettorali;
- **Scambio elettorale politico mafioso (416 ter c.p.)** – Ottenimento della promessa di voti per sé o ad altri in occasione di consultazioni elettorali in cambio dell'erogazione di denaro;
- **Sequestro di persona a scopo di rapina o di estorsione (630 c.p.)** – Sequestro di una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione;
- **Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope** (art. 74 del d.P.R. 9 ottobre 1990, n. 309) – Associazione realizzata da tre o più persone al fine di coltivare, produrre, fabbricare, estrarre, raffinare, vendere, offrire o mettere in vendita, cedere, distribuire, commerciare, trasportare, procurare ad altri, inviare, passare o spedire in transito, consegnare per qualunque scopo sostanze stupefacenti o psicotrope;
- **Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo** (art. 407 c.p.p.)

Con questo intervento legislativo, i delitti di criminalità organizzata diventano presupposto di responsabilità degli enti ex D.Lgs 231/01 anche nei casi in cui tali reati non si configurino come transnazionali.

Per la società sono previste sanzioni pecuniarie da 300 a 1000 quote (da 77 migliaia di Euro a 1.549 migliaia di Euro) e sanzioni interdittive ex art. 9, comma 2 del D.Lgs. n. 231/2001, per una durata non inferiore a un anno.

4.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze.**
- **Stipula e gestione dei rapporti contrattuali con clienti e controparti.**
- **Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi.**

4.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento nonché di assetto del sistema di organizzazione, gestione e controllo che dovranno essere seguite dai Destinatari per prevenire la costituzione di associazioni criminose all'interno della SGR per la commissione di delitti legati all'attività svolta (ad esempio: reati di corruzione, reati tributari, reati societari) e di comportamenti diretti ad agevolare l'attività di associazioni criminali.

A tale scopo, devono essere adottate le seguenti regole generali:

- la scelta di controparti, per la conclusione, sotto qualsiasi forma, di rapporti commerciali, deve avvenire nel rispetto delle procedure aziendali che devono assicurare il rispetto di criteri predeterminati e verificabili. In ogni caso, la selezione avviene preferibilmente nell'ambito di soggetti già accreditati presso la SGR e comunque previa verifica della loro reputazione e affidabilità sul mercato, acquisizione e archiviazione della documentazione;
- sono chiaramente definiti ed identificati i ruoli e le responsabilità dei soggetti e delle funzioni competenti all'elaborazione dei piani di dismissione, acquisizione e sviluppo immobiliare e sono chiaramente descritte le attività assegnate a ciascuna funzione competente;
- l'acquisizione di beni o rami di azienda è effettuata solo previo svolgimento di adeguati accertamenti per verificare la legittima provenienza degli stessi;
- devono essere svolti accertamenti preventivi e commisurati al rischio per verificare la sussistenza in capo ai partner nei rapporti commerciali o al cedente di ramo d'azienda di sentenze di condanne definitive o di procedimenti penali per i reati associativi di cui all'art. 24-ter D. Lgs. 231/2001, ovvero vi sia stata applicazione, o proposta di applicazione, delle misure di prevenzione, personali o patrimoniali, di cui alla l. 575/1965 e successive modifiche.

4.4 Procedure specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi:

4.4.1 Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze

In aggiunta alle disposizioni previste nella Parte Speciale *“REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI”*, in particolare ove concernenti la selezione, valutazione ed approvazioni dei fornitori, sono adottate le seguenti disposizioni:

- i contratti di approvvigionamento, che possano presentare carattere inusuale o anomalo per tipologia o oggetto della richiesta, sono preventivamente valutati e autorizzati dal vertice della SGR;
- in caso di dubbio sulla qualifica o sulla permanenza della qualifica in capo al fornitore oppure in caso di sopravvenienza di profili di anomalia nei rapporti con il fornitore o nella tipologia delle richieste da questi avanzate, il rapporto può essere mantenuto solo con espressa autorizzazione del vertice della SGR;
- i Destinatari segnalano immediatamente all’OdV, oppure al proprio superiore gerarchico, che riferirà all’OdV, eventuali anomalie, di cui vengano a conoscenza, nelle prestazioni dovute dal fornitore, discordanze significative o ripetute tra materiale o servizio ricevuto rispetto a quanto concordato o particolari richieste avanzate dal fornitore alla SGR;

4.4.2 Stipula e gestione dei rapporti contrattuali con clienti e controparti

Si rimanda alla Parte Speciale *“REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI”*, ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

4.4.2 Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi

Si rimanda alla Parte Speciale *“REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI”*, ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi

4.5 Controlli dell’Organismo di Vigilanza

Per la descrizione dei controlli suggeriti per specifici processi, si rimanda a quanto riportato nella Parte Speciale *“REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI”*.

5 REATI ED ILLECITI AMMINISTRATIVI E ABUSO DI MERCATO

5.1 Le fattispecie di reato in materia di illeciti amministrativi e abuso di mercato

Tra i reati di Insider Trading (art.184 TUF) contemplati all'art. 25 *sexies* del Decreto 231, sono ricompresi i seguenti:

- **Manipolazione del mercato (artt. 185 e 187 ter del D.lg. 58/98 Testo Unico della Finanza).**

L'abuso di mercato realizzato attraverso l'alterazione delle dinamiche relative alla corretta formazione del prezzo di strumenti finanziari è punito dall'art. 185 TUF (manipolazione del mercato) sia da un illecito amministrativo, previsto dall'art. 187 ter TUF.

A differenza del caso dell'aggiotaggio, ove vengono in considerazione strumenti finanziari non quotati o per i quali non sia stata presentata domanda di ammissione alla negoziazione in un mercato regolamentato, nel caso del reato e dell'illecito amministrativo di manipolazione del mercato, si tratta di strumenti finanziari quotati per i quali sia stata presentata richiesta di ammissione alla negoziazione su mercati regolamentati.

La condotta costitutiva del reato di manipolazione del mercato consiste:

- nella diffusione di notizie false (*information based manipulation*);
- nel compimento di operazioni simulate o di altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o non quotati (*action based manipulation*).

L'illecito amministrativo di manipolazione del mercato (art. 12 Regolamento UE 596/2014) si configura invece nelle ipotesi di:

a) l'avvio di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra condotta che:

i) invii, o è probabile che invii, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni; oppure ii) consenta, o è probabile che consenta, di fissare il prezzo di mercato di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale;

a meno che la persona che avvia un'operazione, inoltra un ordine di compravendita o ha posto in essere qualsiasi altra condotta stabilisca che tale operazione, ordine o condotta sono giustificati da legittimi motivi e sono conformi a una pratica di mercato ammessa, come stabilito a norma dell'articolo 13;

b) l'avvio di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra attività o condotta che incida, o sia probabile che incida, sul prezzo di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni, utilizzando artifici o qualsiasi altra forma di raggirio o espediente;

c) la diffusione di informazioni tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo, che forniscano, o siano idonei a fornire, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni o che consentano, o è probabile che consentano, di fissare il prezzo di mercato di uno o più strumenti finanziari o di contratti a pronti su merci collegati o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale

o artificiale, compresa la diffusione di voci, quando la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti;

d) la trasmissione di informazioni false o fuorvianti o la comunicazione di dati falsi o fuorvianti in relazione a un indice di riferimento (benchmark) quando la persona che ha proceduto alla trasmissione o fornito i dati sapeva, o avrebbe dovuto sapere, che erano falsi o fuorvianti, ovvero qualsiasi altra condotta che manipola il calcolo di un indice di riferimento.

Le seguenti condotte sono considerate, tra le altre, manipolazione del mercato:

a) la condotta di una o più persone che agiscono in collaborazione per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario, di contratti a pronti su merci collegati o di un prodotto oggetto d'asta

sulla base di quote di emissioni che abbia, o è probabile che abbia, l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o ponga in atto, o è probabile che lo faccia, altre condizioni commerciali non corrette;

b) l'acquisto o la vendita di strumenti finanziari all'apertura o alla chiusura del mercato, con l'effetto o il probabile effetto di fuorviare gli investitori che agiscono sulla base dei prezzi esposti, compresi i prezzi di apertura e di chiusura;

c) l'inoltro di ordini in una sede di negoziazione, comprese le relative cancellazioni o modifiche, con ogni mezzo disponibile di negoziazione, anche attraverso mezzi elettronici, come le strategie di negoziazione algoritmiche e ad alta frequenza, e che esercita uno degli effetti di cui al paragrafo 1, lettere a) o b), in quanto:

i) interrompe o ritarda, o è probabile che interrompa o ritardi, il funzionamento del sistema di negoziazione della sede di negoziazione;

ii) rende più difficile per gli altri gestori individuare gli ordini autentici sul sistema di negoziazione della sede di negoziazione, o è probabile che lo faccia, anche emettendo ordini che risultino in un sovraccarico o in una destabilizzazione del book di negoziazione (order book) degli ordini; oppure

iii) crea, o è probabile che crei, un segnale falso o fuorviante in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, in particolare emettendo ordini per avviare o intensificare una tendenza;

c) trarre vantaggio da un accesso occasionale o regolare ai mezzi di informazione tradizionali o elettronici diffondendo una valutazione su uno strumento finanziario, un contratto a pronti su merci collegato o un prodotto oggetto d'asta sulla base di quote di emissioni (o indirettamente sul suo emittente) dopo aver precedentemente preso delle posizioni su tale strumento finanziario, contratto a pronti su merci collegato o prodotto oggetto d'asta sulla base di quote di emissioni, beneficiando successivamente dell'impatto della valutazione diffusa sul prezzo di detto strumento, contratto a pronti su merci collegato o prodotto oggetto d'asta sulla base di quote di emissioni, senza aver contemporaneamente comunicato al pubblico, in modo corretto ed efficace, l'esistenza di tale conflitto di interessi;

e) l'acquisto o la vendita sul mercato secondario, in anticipo sull'asta tenuta ai sensi del regolamento (UE) n. 1031/2010, di quote di emissioni o dei relativi strumenti derivati, con

l'effetto di fissare il prezzo di aggiudicazione dell'asta a un livello anormale o artificiale o di indurre in errore gli altri partecipanti all'asta.

Abuso di informazioni privilegiate (art. 184 e 187 bis del D.lg. 58/98 Testo Unico della Finanza).

Le norme in esame puniscono l'abuso delle informazioni privilegiate conosciute in ragione dell'attività svolta attraverso il compimento di operazioni sugli strumenti finanziari cui le informazioni si riferiscono, ovvero attraverso la comunicazione – in forma diretta o indiretta – di dette informazioni.

1. È punito con la reclusione da due a dodici anni e con la multa da euro ventimila a euro tre milioni chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente ovvero dell'esercizio di un'attività lavorativa, di una professione o 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;

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'articolo 11 del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014;

c) raccomanda o induce altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate nella lettera a).

2. La stessa pena si applica a chiunque, essendo in possesso di informazioni privilegiate a motivo della preparazione o dell'esecuzione di attività delittuose, commette taluno dei fatti di cui al comma 1.

3. Fuori dei casi di concorso nei reati di cui ai commi 1 e 2, è punito con la reclusione da un anno e sei mesi a dieci anni e con la multa da euro ventimila a euro due milioni e cinquecentomila chiunque, essendo in possesso di informazioni privilegiate per ragioni diverse da quelle indicate ai commi 1 e 2 e conoscendo il carattere privilegiato di tali informazioni, commette taluno dei fatti di cui al comma 1.

Nei casi di cui ai commi 1, 2 e 3, la pena della multa può essere aumentata fino al triplo o fino al maggior importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

Le disposizioni del presente articolo 184 del TUF si applicano anche quando i fatti di cui ai commi 1, 2 e 3 riguardano condotte od 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 della Commissione, del 12 novembre 2010).

Per informazione privilegiata si intende:

a) 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;

b) in relazione agli strumenti derivati su merci, un'informazione avente un carattere preciso, che non è stata comunicata al pubblico, concernente, direttamente o indirettamente, uno o più di tali strumenti derivati o concernente direttamente il contratto a pronti su merci collegato, e che, se comunicata al pubblico, potrebbe avere un effetto significativo sui prezzi di tali strumenti derivati o sui contratti a pronti su merci collegati e qualora si tratti di un'informazione che si possa ragionevolmente attendere sia comunicata o che debba essere obbligatoriamente comunicata conformemente alle disposizioni legislative o regolamentari dell'Unione o nazionali, alle regole di mercato, ai contratti, alle prassi o alle consuetudini, convenzionali sui pertinenti mercati degli strumenti derivati su merci o a pronti;

c) in relazione alle quote di emissioni o ai prodotti oggetto d'asta correlati, un'informazione avente un carattere preciso, che non è stata comunicata al pubblico, concernente, direttamente o indirettamente, uno o più di tali strumenti e che, se comunicata al pubblico, potrebbe avere un effetto significativo sui prezzi di tali strumenti o sui prezzi di strumenti finanziari derivati collegati;

d) nel caso di persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, s'intende anche l'informazione trasmessa da un cliente e connessa agli ordini pendenti in strumenti finanziari del cliente, avente un carattere preciso e concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari e che, se comunicata al pubblico, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari, sul prezzo dei contratti a pronti su merci collegati o sul prezzo di strumenti finanziari derivati collegati.

5.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Reporting e Marketing.**

I Destinatari sono tenuti a osservare i presidi organizzativi aziendali di seguito esposti in riferimento a ciascuna attività a rischio-reato, le previsioni legislative esistenti in materia e i principi contenuti nel Codice Interno di Comportamento. Il Personale della SGR, a qualsiasi titolo coinvolto nelle attività a rischio-reato identificate, è inoltre tenuto a rispettare le disposizioni ed eseguire i controlli di competenza formalizzati nella normativa interna di volta in volta rilevante e nell'ulteriore documentazione adottata in attuazione del sistema dei controlli e dei principi di comportamento contenuti nella presente Parte Speciale.

5.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 5.1.

All'uopo, è fatto espresso divieto di:

- comunicare le informazioni privilegiate a terzi per ragioni diverse da quelle di ufficio (a titolo esemplificativo e non esaustivo: clienti, emittenti di titoli pubblicamente contrattati, ecc.) ovvero raccomandare o indurre terzi a compiere operazioni connesse alle informazioni privilegiate; qualora dette informazioni debbano essere comunicate a terzi (consulenti e/o professionisti esterni) per ragioni di ufficio, è fatto obbligo di accertare che costoro siano soggetti ad un obbligo di riservatezza legale, regolamentare o statutario; in difetto è necessario formalizzare, mediante sottoscrizione di un accordo di *confidentiality*, il reciproco dovere di riservatezza circa le informazioni scambiate;
- 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; particolare attenzione deve essere prestata nell'uso di telefoni cellulari e di telefoni "viva voce", onde evitate che le informazioni privilegiate possano essere ascoltate da estranei o comunque da soggetti che non hanno necessità di conoscerle;
- comunicare al mercato o ai media informazioni privilegiate relative alle società clienti della SGR; qualora fosse richiesto un commento su specifiche operazioni relative a tali emittenti, ci si dovrà limitare a commentare i fatti già resi pubblici dall'emittente in base all'art. 114 del TUF; in ogni caso, sono previsti obblighi di consultazione con le strutture/funzioni aziendali che sono legittimamente in possesso delle informazioni privilegiate;
- diffondere sia ad altro personale sia all'esterno della SGR, attraverso qualsiasi canale informativo, compreso internet, 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 in relazione alla SGR e/o ai relativi strumenti finanziari nonché in relazione a società terze in rapporto d'affari con la SGR;
- produrre e diffondere studi e ricerche in violazione delle norme, interne ed esterne, specificamente dettate per tale attività e, in particolare, senza comunicare nei modi richiesti dalla normativa gli interessi rilevanti e/o i conflitti eventualmente sussistenti.

È fatto obbligo:

- di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la SGR e gli strumenti finanziari della stessa, sia riguardanti società terze in rapporto d'affari con la SGR e gli strumenti finanziari di queste ultime nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- secondo quanto stabilito dalle norme interne in tema di sicurezza fisica e logica, 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.

5.4 Procedure specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate dalla SGR.

5.4.1 Reporting e attività di marketing

La SGR adotta una specifica Procedura in materia trattamento delle informazioni privilegiate con cui si definiscono gli obblighi in materia di riservatezza sulle informazioni privilegiate o confidenziali acquisite dagli investitori o dai clienti ovvero di cui comunque abbiano avuto conoscenza nello svolgimento della propria attività.

La SGR adotta altresì specifiche procedure in materia di operazioni personali. Nelle procedure aziendali sono stati identificati e individuati i soggetti considerati rilevanti per la SGR, ai quali è fatto divieto di effettuare operazioni, anche per interposta persona, nell'interesse proprio o di terzi ovvero di consigliare, sollecitare qualsiasi altra persona, al di fuori dell'ambito normale della propria attività lavorativa o di un contratto di esternalizzazione ad effettuare operazioni i) che costituiscono abuso di informazioni privilegiate o manipolazioni di mercato; ii) che implicano l'abuso di informazioni o la divulgazione scorretta di informazioni confidenziali.

La SGR altresì alimenta e aggiorna una specifica Mappatura delle Parti Correlate.

Le procedure attribuiscono alla Funzione Compliance un'attività di monitoraggio e verifica, svolta sia in via diretta sia tramite le strutture aziendali.

L'Ufficio Amministrazione e Finanza riceve e conserva i) le comunicazioni delle operazioni effettuate dai Soggetti Rilevanti e/o dalle persone strettamente legate ai Soggetti Rilevanti; ii) le dichiarazioni con le quali i Soggetti Rilevanti danno atto della piena conoscenza ed accettazione della normativa vigente;

Il Responsabile della Funzione Compliance raccoglie le segnalazioni sulle violazioni e, mantenendo assoluta riservatezza sull'identità del segnalante provvede ai necessari accertamenti e ad attivare le azioni conseguenti;

Sono mantenuti costantemente aggiornati sistemi di sicurezza logica e fisica a garanzia della corretta gestione delle informazioni.

Sono previste modalità di trasmissione, conservazione e archiviazione della documentazione contenente informazioni confidenziali o privilegiate volte a garantirne la riservatezza;

Gli atti ed i documenti di pertinenza della SGR, o nella sua disponibilità, che contengano informazioni privilegiate e confidenziali sono custoditi in luoghi e armadi sicuri, tenuti sotto chiave quando non utilizzati. Tali atti e documenti, ove presenti in archivi informatici, devono essere protetti per mezzo di accessi personalizzati;

Gli atti e i documenti di pertinenza della SGR, o nella sua disponibilità, che contengano informazioni privilegiate e confidenziali possono essere portati fuori dei locali della stessa unicamente per motivi strettamente connessi all'attività della SGR.

5.5 Controlli dell'Organismo di Vigilanza

Con riferimento ai processi a rischio identificati, l'Organismo di Vigilanza ha il compito di:

- valutare l'efficacia e monitorare il rispetto dei principi definiti nel presente Modello, nel Codice Interno di Comportamento e nelle Procedure Aziendali in materia di informazioni privilegiate e operazioni personali;

- verificare la corretta tenuta del Registro delle persone che hanno accesso alle Informazioni Privilegiate e Rilevanti;
- promuovere iniziative di formazione / informazione periodica relativamente ai reati ed agli illeciti amministrativi di abuso di mercato e dei relativi regolamenti/procedure aziendali.

6. REATI CON FINALITÀ DI TERRORISMO

6.1 Le fattispecie di reato con finalità di terrorismo

Gli artt. 25 quater e 25 quater 1 del D.Lgs. 231/2001 **Delitti con finalità di terrorismo o di eversione dell'ordine democratico** comprendono i seguenti reati previsti dal codice penale:

- Associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (**Art. 270 bis c.p.**)
- Assistenza agli associati (**Art. 270 ter c.p.**)
- Arruolamento con finalità di terrorismo anche internazionale (**Art. 270 quater c.p.**)
- Addestramento con finalità di terrorismo anche internazionale (**Art. 270 quinquies c.p.**)
- Condotte con finalità di terrorismo (**Art. 270 sexies c.p.**)
- Attentato con finalità terroristiche o di eversione (**Art. 280 c.p.**)
- Atto di terrorismo con ordigni micidiali o esplosivi (**Art. 280 bis c.p.**)
- Sequestro di persona a scopo di terrorismo o di eversione (**Art. 289 bis c.p.**)
- Istigazione a commettere alcuno dei delitti previsti dai capi primo e secondo (**Art. 302 c.p.**)

Inoltre, l'art. 8 della Legge n. 7 del 9 gennaio 2006, riguardante le "Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile" ha introdotto all'interno della normativa sulla Responsabilità amministrativa il reato di pratiche di mutilazione degli organi genitali femminili previsto dal codice penale (art. 583 bis c.p.).

Si applicano sia sanzioni amministrative che interdittive.

Alla Società, nella cui struttura è commesso il delitto, si applica la sanzione pecuniaria da 200 a 700 quote se il delitto è punito con la reclusione inferiore a 10 anni, oppure da 400 a 1000 quote se punito con reclusione superiore a 10 anni.

6.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze;**
- **Stipula e gestione dei rapporti contrattuali con clienti e controparti;**
- **Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi.**

La prevenzione dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico si fonda sul rispetto, da parte della SGR, delle norme dettate per gli intermediari da Banca d'Italia (Unità di

Informazione Finanziaria) in materia di antiriciclaggio e di segnalazioni di operazioni finanziarie sospette.

Il rischio che siano posti in essere i reati con finalità di terrorismo e di eversione dell'ordine democratico e i reati contro la persona riguarda principalmente le attività di instaurazione dei rapporti con la clientela e con le controparti, attività che, ai fini della prevenzione dei reati in questione, si devono basare sul fondamentale principio dell'adeguata conoscenza della clientela. Tale principio rappresenta uno dei principali presupposti stabiliti dal D. Lgs. n. 231/2007 concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminosi e di finanziamento del terrorismo.

In particolare, la normativa in tema di finanziamento del terrorismo è incentrata sul decreto legislativo 22 giugno 2007 n. 109 che regola le modalità operative per eseguire le misure di congelamento di fondi e di risorse economiche stabilite:

- dalle Risoluzioni del Consiglio di sicurezza delle Nazioni Unite;
- dai regolamenti comunitari (c.d. "sanzioni finanziarie internazionali") per il contrasto del finanziamento del terrorismo e dei Paesi che minacciano la pace e la sicurezza internazionale.

Gli obblighi a carico della SGR consistono in:

- Misure del congelamento di fondi e di risorse economiche
- Obblighi di comunicazione all'Unità di Informazione Finanziaria le misure di congelamento
- Obblighi di segnalazione all'Unità di Informazione Finanziaria delle operazioni sospette di riciclaggio alle operazioni ed ai rapporti che, in base alle informazioni disponibili, possano essere riconducibili ad attività di finanziamento del terrorismo.

Per quanto precede, si individua quale attività sensibile in cui potrebbero presentarsi potenziali rischi per la commissione dei reati sopra illustrati l'attività aziendale sensibile inerente al contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminosi.

6.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

Con riferimento ai reati in considerazione, è fatto divieto ai componenti degli organi sociali e ai dipendenti della SGR di effettuare operazioni con chiunque senza la preventiva fase d'istruttoria relativa all'identificazione ed alla valutazione dei nuovi clienti della e delle attività da essi svolte.

Analoghe procedure di identificazione e valutazione devono essere adottate anche nelle fasi istruttorie relativamente ai processi di assunzione del personale e dei collaboratori e di acquisizione di nuovi fornitori.

A tal fine sono adottati idonei presidi volti ad assicurare la verifica puntuale delle apposite liste comunitarie ed internazionali contenenti i nominativi dei soggetti sottoposti a sanzioni finanziarie volte a contrastare e prevenire fenomeni di finanziamento del terrorismo.

Inoltre, sempre ai fini della prevenzione dei reati sopra citati, tutti i dipendenti dovranno attenersi alle Procedure formalizzate per l'identificazione dei clienti, per la selezione dei fornitori e per l'esecuzione

di ordini di pagamento, anche avvalendosi di elenchi/applicativi contenenti nominativi di soggetti coinvolti (o potenzialmente coinvolti) in attività terroristiche e dovranno segnalare tutte le operazioni sospette come da Procedure aziendali.

6.4 Procedure Specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi.

6.4.1 Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze

Si rimanda alle Parti Speciali “REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI” e “REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO BENI O UTILITA’ DI PROVENIENZA ILLECITA NONCHE’ AUTORICICLAGGIO” ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

6.4.2 Stipula e gestione dei rapporti contrattuali con clienti e controparti

Si rimanda alle Parti Speciali “REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI” e “REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO BENI O UTILITA’ DI PROVENIENZA ILLECITA NONCHE’ AUTORICICLAGGIO” ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

6.4.3 Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi

Si rimanda alle Parti Speciali “REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI” e “REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO BENI O UTILITA’ DI PROVENIENZA ILLECITA NONCHE’ AUTORICICLAGGIO” ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

6.5 Controlli dell’Organismo di Vigilanza

Per la descrizione dei controlli suggeriti per specifici processi, si rimanda a quanto riportato nella Parte Speciale *“REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITA’ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI”*.

7. REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

7.1 Le fattispecie di reati in tema di salute e sicurezza sul lavoro

I reati presupposto contenuti nella presente sezione sono disciplinati dall'articolo 25 *septies* del Decreto:

- **Omicidio colposo (art. 589 c.p.)**

L'art. 25 *septies*, primo comma, del Decreto introduce, quale reato sanzionato ai sensi del Decreto stesso, il delitto di omicidio colposo commesso con violazione dell'articolo 55, comma 22, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, ovvero del D.Lgs. n. 81/2008.

L'art. 25 *septies*, secondo comma, sanziona altresì il delitto di omicidio colposo di cui all'art. 589 del Codice Penale qualora esso sia commesso, in generale, con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Ai sensi dell'art. 589 del Codice Penale, commette tale fattispecie di reato "chiunque cagiona per colpa la morte di una persona"; ai sensi del terzo comma del detto articolo, costituisce circostanza aggravante l'aver commesso il fatto con violazione delle "norme per la prevenzione degli infortuni sul lavoro".

Tale ipotesi di reato potrebbe configurarsi nel caso in cui la violazione colposa delle norme sulla tutela della sicurezza e salute sul lavoro, adottate in azienda, determini un incidente sul lavoro che cagioni la morte di un dipendente della SGR.

Ad esempio, in ipotesi di morte a seguito di un incendio divampato nei locali aziendali a causa di un cortocircuito del sistema informatico, in relazione al quale era stata negligenza omessa, da parte dei soggetti aziendali a ciò preposti, la periodica verifica di funzionalità e sicurezza.

- **Lesioni personali colpose gravi e gravissime (art. 590 c.p.)**

L'art. 25 *septies* introduce altresì, quale reato sanzionato dal Decreto, il delitto di lesioni personali colpose di cui all'articolo 590, terzo comma, del Codice Penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Ai sensi dell'art. 590 del Codice Penale, commette tale fattispecie di reato "chiunque cagiona ad altri, per colpa, una lesione personale"; costituisce circostanza aggravante, ai sensi del terzo comma del detto articolo, il fatto di aver cagionato la lesione personale con violazione delle "norme per la prevenzione degli infortuni sul lavoro".

² Tale ultima disposizione stabilisce che, nei casi previsti dall'art. 55, comma 1, lett. a) del D.Lgs. n. 81/2008, ovvero nelle ipotesi in cui il datore di lavoro omette la valutazione dei rischi e l'adozione del documento di cui all'art. 17, comma 1, lett. a), ovvero lo adotta in assenza degli elementi di cui alle lettere a), b), d) ed f) dell'art. 28, e viola le disposizioni di cui all'art. 18, comma 1, lett. q) e z) prima parte, si applica la pena dell'arresto da sei mesi a un anno e sei mesi se la violazione è commessa:

a) nelle aziende di cui all'art. 31, comma 6, lett. a, b, c, d, f, ovvero:

- aziende industriali di cui all'art. 2 del D.Lgs. 334/99, soggette all'obbligo di notifica o rapporto;

- nelle centrali termoelettriche;

- negli impianti ed installazioni nucleari o che impiegano a qualsiasi titolo materiale radioattivo o che smaltiscono rifiuti radioattivi (D.Lgs. 230/1995, artt. 7, 28 e 33);

- nelle aziende per la fabbricazione e il deposito separato di esplosivi, polveri e munizioni;

- nelle industrie estrattive con oltre 50 lavoratori.

b) nelle aziende che svolgono attività che espongono i lavoratori a rischi biologici "gravi" (art. 268, I comma, lett. c e d), da atmosfere esplosive, cancerogeni mutanti e da attività di manutenzione, rimozione, smaltimento e bonifica di amianto;

c) per le attività disciplinate dal titolo IV ("cantieri temporanei o mobili") del D.Lgs. n. 81/2008 e caratterizzate dalla compresenza di più imprese e la cui entità presunta di lavoro non sia inferiore a 200 uomini-giorno.

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.

Tale ipotesi di reato potrebbe configurarsi nel caso in cui la violazione colposa delle norme sulla tutela della sicurezza e salute sul lavoro determini un incidente sul lavoro che cagioni a un dipendente della SGR una lesione personale grave ovvero gravissima.

Ad esempio, qualora un dipendente della SGR subisca delle lesioni in seguito ad una caduta addebitabile alla presenza di arredo non a norma nei locali aziendali.

La persona fisica che commette il reato di omicidio colposo è punita con la reclusione da uno a dodici anni, diversamente la persona fisica che commette il reato di lesioni personali colpose gravi o gravissime è punita con la reclusione da due mesi a cinque anni.

Per la Società sono previste sanzioni pecuniarie (a partire da 10 mila Euro) e sanzioni interdittive non inferiori a tre mesi e fino ad un anno.

7.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- Gestione degli adempimenti in materia di salute e sicurezza sul lavoro

Il Datore di lavoro è il principale garante della sicurezza all'interno dell'azienda (artt. 17 e 18 D.Lgs. 81/2008) e si avvale di altre figure aziendali (Dirigenti e Preposti) o esterne (RSPP) per l'attuazione ed il corretto funzionamento del sistema di gestione della salute e della sicurezza sul luogo di lavoro. Sono tuttavia da considerare come coinvolti nella gestione dei rischi in materia di salute e sicurezza sul lavoro tutti Dipendenti, collaboratori, Appaltatori, a prescindere dalla loro collocazione, dalla forma della loro collaborazione con la società, dalle loro mansioni svolte, dal loro livello gerarchico, in quanto sono obbligati a svolgere le loro attività nel rispetto del sistema delle regole e norme di riferimento, e ad adempiere agli obblighi e a rispettare le prescrizioni e divieti definiti nel suddetto sistema.

Il sistema di regole e norme in materia di salute e sicurezza sul lavoro è composto dai principi generali di condotta e comportamento e dai principi specifici definiti nei paragrafi del presente Capitolo, sia dalla normativa vigente e dalle norme/linee guida a riguardo.

Le prescrizioni contenute

- nel Decreto Legislativo 9 aprile 2008, n. 81;
- nella norma BS OHSAS 18001:2007 o UNI 45001:2018.

sono quindi da considerarsi complementari a quelle esplicitamente previste nel presente Modello.

Oltre agli aspetti trasversali del processo, come illustrato sopra, la gestione dei rischi in materia di salute e sicurezza sul lavoro prevede anche delle attività specifiche, demandate a figure aziendali individuate per ogni luogo di lavoro e a cui sia stato attribuito un ruolo specifico in materia di salute e sicurezza sul lavoro (con il supporto di altri soggetti aziendali o esterni, ove necessario/opportuno).

Questo processo può essere suddiviso nelle seguenti fasi e attività specifiche:

- Identificazione dei pericoli per la sicurezza e per la salute dei lavoratori;
- classificazione dei pericoli;
- Valutazione dei rischi [anche da interferenza];
- Individuazione delle misure di prevenzione e di protezione;
- Definizione di un piano di intervento di attuazione delle misure di prevenzione e di protezione;
- Realizzazione degli interventi pianificati.
- Attività di monitoraggio e controllo.

7.3 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta generali e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti.

Ciascuna decisione aziendale che possa avere riflessi sulle condizioni di lavoro deve prevedere una preliminare valutazione delle tematiche connesse alla sicurezza e alla salute del lavoro, individuando la compatibilità con l'assetto esistente, ovvero la necessità di intraprendere azioni di adeguamento;

Devono essere destinate risorse umane e finanziarie adeguate ai fini dell'implementazione di un sistema di prevenzione dei rischi in materia di salute e sicurezza nei luoghi di lavoro conforme alle disposizioni normative vigenti.

Tutti i Destinatari sono tenuti a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela;
- astenersi dall'affidare incarichi a consulenti/professionisti esterni eludendo criteri documentabili ed obiettivi quali professionalità qualificata e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, ecc.) in occasione di accertamenti/procedimenti ispettivi;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nei confronti di tutto il personale;
- assicurarsi che, nell'impiego di sistemi di elaborazione automatica dei dati, le modalità di memorizzazione dei dati e di accesso al sistema di gestione della documentazione prescritta garantiscano quanto previsto dall'art. 53 del Testo Unico della Sicurezza;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, con espresso divieto di manomettere o interdire i dispositivi di sicurezza;

- segnalare immediatamente al proprio responsabile e/o agli addetti alla gestione delle emergenze, ogni situazione di pericolo potenziale o reale, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo.

Tutti dipendenti e collaboratori di GRADIENTE, sono tenuti a:

- rispettare le norme, gli obblighi e i principi posti dalla normativa vigente e dalle norme/linee guide in materia di salute e sicurezza contenute nel Decreto Legislativo 9 aprile 2008, n. 81 e nella norma BS OHSAS 18001:2007 o [UNI 45001:2018](#);
- rispettare i principi generali di condotta e comportamento, i principi di controllo e i principi specifici formulati nel presente Modello 231;
- promuovere il rispetto delle suddette norme, regole e principi ed assicurare gli adempimenti in materia di salute e sicurezza sul lavoro;
- adottare una condotta di massima collaborazione e trasparenza e rispettare i principi di condotta e comportamento specificati nel Capitolo relativo ai rapporti con gli enti pubblici competenti in materia salute e sicurezza sul lavoro, sia in fase di stesura e comunicazione di eventuali dichiarazioni, sia in occasione di accertamenti/verifiche ispettive;
- promuovere l'informazione e formazione interna in tema di rischi specifici connessi allo svolgimento delle proprie mansioni e attività, di struttura e regolamento aziendale in materia di salute e sicurezza, procedure e misure di prevenzione e protezione e/o prendere atto dell'informazione fornita e/o partecipare attivamente ai corsi di formazione;
- utilizzare correttamente i macchinari, le apparecchiature, gli impianti, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- segnalare ai Responsabili o ai soggetti responsabili per la gestione della salute e sicurezza e/o all'OdV (attraverso l'invio di una Segnalazione da effettuarsi nelle circostanze e secondo le modalità definite nell'ambito della Parte Generale) violazioni delle norme definite, inefficacia dei mezzi di prevenzione e protezione ed ogni situazione di pericolo potenziale o reale.

7.4 Procedure Specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi.

7.4.1 Gestione dei rischi in materia di salute e sicurezza sul lavoro

I soggetti che esercitano poteri autorizzativi e/o negoziali sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal vigente sistema dei poteri e delle deleghe della SGR.

La SGR adotta una politica aziendale di salute e sicurezza quale valore aziendale che caratterizza la strategia d'impresa da conseguire ed implementare costantemente, con l'ausilio di un sistema organizzativo che ne individui, in particolare, gli strumenti, le procedure e le responsabilità.

Il Datore di Lavoro, in qualità di principale garante della sicurezza all'interno della SGR, è tenuto agli obblighi indicati nell'art. 18 del Testo Unico Sicurezza, avvalendosi anche dell'istituto della delega di funzioni ai sensi dell'art. dall'art. 16 del Testo Unico Sicurezza, fatta eccezione per l'attività indelegabili.

Il Responsabile del Servizio Prevenzione e Protezione coordina le strutture operative che hanno il compito di realizzare e gestire gli interventi (di natura immobiliare, di sicurezza fisica, ovvero attinenti a processi di lavoro e alla gestione del personale), che sono distinte e separate dalla struttura alla quale sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;

Sono designati soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;

I soggetti individuati ai sensi della normativa in materia rappresentano figure che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati alla natura dell'incarico loro conferito, attuano le direttive del Datore di Lavoro, organizzando l'attività lavorativa e vigilando su di essa.

I Preposti sono individuati ai sensi della normativa in materia:

- sovrintendono e vigilano sull'osservanza da parte dei lavoratori degli obblighi di legge e delle misure di protezione e di prevenzione, compresi i dispositivi di protezione individuale;
- informano il Datore di Lavoro o il loro superiore diretto di eventuali persistenti inosservanze;
- informano i lavoratori esposti ad un rischio di un pericolo grave e immediato in ordine all'entità del rischio e alle disposizioni da osservare;
- avvertono tempestivamente il Datore di Lavoro delle deficienze dei mezzi di protezione e di ogni altra condizione di pericolo, che si verifichino durante il lavoro;
- si accertano che, in caso di emergenza, i lavoratori osservino le misure predisposte, fornendo istruzioni in ordine alle modalità per l'abbandono del posto di lavoro;

Il Rappresentante dei Lavoratori per la Sicurezza collabora attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni.

Sono previste idonee attività di gestione sistematica del rischio attraverso:

- individuazione e determinazione delle misure di prevenzione e di protezione attuate e i dispositivi di protezione individuale;
- individuazione di procedure per l'attuazione delle misure e di figure aziendali coinvolte in questo processo;
- programmazione delle misure più idonee a garantire il miglioramento nel tempo dei livelli di sicurezza;
- individuazione ed organizzazione delle procedure di emergenza e di primo soccorso.

Le strutture competenti attivano in particolare un piano aziendale di controllo sistematico al fine di verificare periodicamente la corretta applicazione/gestione, nonché l'efficacia delle procedure adottate e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro.

Il piano aziendale deve assicurare:

- il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- l'acquisizione di documentazioni e certificazioni obbligatorie di legge (relative ad edifici, impianti persone, società ecc.) da parte delle competenti strutture;

- il rispetto del processo e degli adempimenti tecnici ed amministrativi previsti dalle norme interne e di legge;
- un idoneo sistema di controllo sulla sua efficace attuazione e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

La SGR prevede un'attività di riesame ed eventuale modifica del piano qualora siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

Tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente ed il Responsabile del Servizio Prevenzione e Protezione visitano tutti i luoghi di lavoro;

Sono pianificate le attività di informazione e di formazione previste dalla normativa vigente.

Al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura/funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, ivi compresa la documentazione comprovante i requisiti tecnico-professionali delle imprese appaltatrici, dei lavoratori autonomi e dei soggetti destinatari di deleghe in materia di sicurezza, nonché documentazioni e certificazioni obbligatorie di legge.

Con specifico riferimento all'emergenza pandemica *Covid 19*, per ciò che riguarda la Società, le misure hanno riguardato in primis la tutela della salute e della sicurezza del personale e dei collaboratori. In tale contesto la SGR ha prontamente adottato in conformità alle misure governative di volta in volta vigenti, modalità operative delocalizzate (i.e. "*smart working*") mediante accesso da remoto alla base informativa aziendale ed utilizzo di strumenti di video/teleconferenza che si sono rilevati pienamente funzionali alla prosecuzione dell'operatività ordinaria. In linea con il Protocollo Condiviso Nazionale del 24 aprile 2020, la SGR aveva definito un protocollo interno di sicurezza di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 da adottare per il rientro in ufficio e anche per eventuali accessi saltuari, con la costituzione di un Comitato Emergenza Covid per l'applicazione e la verifica delle regole del protocollo di sicurezza che si riunisce periodicamente.

7.5 Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha facoltà discrezionale di porre in essere le attività di controllo periodico sulle attività aziendali potenzialmente a rischio di commissione dei reati contrari alla sicurezza sul lavoro; tali controlli sono volti a verificare la corretta esplicazione delle regole definite nel Modello e, in particolare, delle procedure interne in essere.

A questo fine, l'Organismo di Vigilanza provvede a:

- monitorare l'efficacia ed il rispetto delle procedure specifiche volte alla prevenzione dei reati contrari alla sicurezza sul lavoro;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo interno o da qualsiasi dipendente o soggetto esterno ed effettuare degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.

- verificare periodicamente il libro infortuni della SGR ed indagare le cause e la gestione di eventuali infortuni occorsi;
- monitorare l'efficacia dei controlli, effettuati dal Responsabile del Sistema di Prevenzione e Protezione per verificare la corretta implementazione del modello di gestione della salute e della sicurezza;
- sollecitare l'aggiornamento tempestivo del modello di gestione della salute e della sicurezza sulla base delle evoluzioni normative, ovvero alla luce delle risultanze delle riunioni periodiche sulla sicurezza;
- verificare la frequenza delle iniziative di formazione – informazione periodica relativamente ai reati legati alla sicurezza sul lavoro.

8. REATI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

8.1 Le fattispecie di reato in materia di strumenti di pagamento diversi dai contanti

L'art. 25-*octies*.1 del Decreto estende la responsabilità amministrativa degli enti ai reati di:

- **art. 493-ter c.p. "Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti" (sanzione pecuniaria tra 300 e 800 quote);**
- **art. 493-quater "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti" (sanzione pecuniaria sino a 500 quote);**
- **art. 640-ter "Frode informatica", non solo se commesso ai danni dello Stato o di altro ente pubblico o dell'Unione Europea, come già previsto dall'art. 24 del Decreto, ma anche "nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale.**

8.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Direzione, sviluppo ed il controllo dei sistemi informativi a supporto dell'operatività della SGR**

Le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti costituiscono una minaccia alla sicurezza in quanto rappresentano fonti di entrate per la criminalità organizzata e quindi rendono possibili altre attività criminali come il terrorismo, il traffico di droga e la tratta di esseri umani. Negli ultimi anni si è verificata non soltanto una crescita esponenziale dell'economia digitale, ma anche una proliferazione dell'innovazione in numerosi settori, tra cui quello delle tecnologie di pagamento. Le nuove tecnologie di pagamento comportano l'uso di nuovi tipi di strumenti di pagamento, che da un lato creano nuove opportunità per i consumatori e le imprese, ma dall'altro aumentano anche le opportunità di frode.

Il concetto di strumento di pagamento diverso dai contanti dovrebbe essere inteso nel senso che lo strumento pone il titolare o l'utente dello strumento nella posizione di permettere realmente un trasferimento di denaro o valore monetario o di iniziare un ordine di pagamento.

Ad esempio, ottenere illecitamente un'applicazione per pagamenti tramite dispositivo mobile senza la necessaria autorizzazione non dovrebbe essere considerato un ottenimento illecito di uno strumento di pagamento diverso dai contanti, in quanto non permette realmente all'utente di trasferire denaro o valore monetario.

Condotte come la raccolta e il possesso di strumenti di pagamento allo scopo di commettere frodi, ad esempio mediante il phishing, lo skimming, oppure indirizzando o reindirizzando gli utenti di un servizio di pagamento verso siti web falsi, e la loro distribuzione, ad esempio vendendo su Internet informazioni relative alle carte di credito, dovrebbero essere qualificate come un reato a sé stante, indipendentemente dal requisito di un'utilizzazione fraudolenta dei mezzi di pagamento diversi dai contanti. Pertanto, tali condotte criminali dovrebbero includere anche i casi in cui il possesso, l'ottenimento o la distribuzione non portino necessariamente all'utilizzazione fraudolenta di tali strumenti di pagamento.

8.3 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo

GRADIENTE adotta tutte le misure necessarie affinché le seguenti condotte, se commesse intenzionalmente, siano punibili come reato:

- a) l'utilizzazione fraudolenta di uno strumento di pagamento diverso dai contanti rubato o altrimenti illecitamente ottenuto ovvero oggetto di illecita appropriazione;
- b) l'utilizzazione fraudolenta di uno strumento di pagamento diverso dai contanti contraffatto o falsificato.

In via generale GRADIENTE adotta azioni adeguate per sensibilizzare i propri dipendenti e collaboratori nonché i propri clienti e ridurre il rischio che le persone diventino vittime di frodi.

8.4 Procedure specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi.

8.4.1 Direzione, sviluppo ed il controllo dei sistemi informativi a supporto dell'operatività della SGR

Quanto definito dal presente paragrafo si applica ai Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione dei rapporti con le Autorità di Vigilanza in occasione di adempimenti, comunicazioni, anche attraverso l'utilizzo della PEC, e visite ispettive, previsti dalla normativa di riferimento.

La SGR mantiene la tracciabilità degli strumenti informatici – che rimangono di esclusiva proprietà dell'azienda - assegnati ai propri dipendenti e ne verifica preventivamente le caratteristiche tecniche, le configurazioni e gli accessi alla rete aziendale;

L'utilizzo dei sistemi informatici da parte dei soggetti assegnatari dev'essere conforme alle politiche ed alle procedure adottate dall'azienda per assicurarne un adeguato livello di protezione;

La SGR assicura il corretto impiego e la regolare funzionalità della posta elettronica e della rete internet definendo le modalità d'uso consentite nello svolgimento dell'attività lavorativa;

I dati, le informazioni ed i documenti dei quali si viene a conoscenza nello svolgimento delle proprie mansioni, devono essere utilizzati esclusivamente per motivi di ufficio e gestiti nel rispetto delle politiche e delle procedure aziendali, nonché delle deleghe e delle procure, volte ad assicurare un'adeguata gestione e protezione degli stessi.

Ad integrazione di quanto sopra si richiama quanto già previsto nella Parte Speciale “*REATI DI CRIMINALITA' INFORMATICA*” ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

8.5 Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha facoltà discrezionale di porre in essere le attività di controllo periodico sulle attività aziendali potenzialmente a rischio di commissione dei reati legati all'utilizzo di strumenti di pagamento diversi dai contanti. Tali controlli sono volti a verificare la corretta esplicazione delle regole definite nel Modello e, in particolare, delle procedure interne in essere.

A questo fine, l'Organismo di Vigilanza provvede a:

- valutare l'efficacia e monitorare il rispetto dei principi definiti nel presente Modello, nel Codice Interno di Comportamento e nelle Procedure Aziendali in materia di utilizzo di strumenti di pagamento diversi dai contanti.

9. REATI DI RICICLAGGIO

9.1 Le fattispecie di reati di ricettazione, riciclaggio, impiego di denaro, beni ed utilità di provenienza illecita, nonché autoriciclaggio

L'art. 63 del D.Lgs. 231/2007, “Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione”, ha introdotto l'art. 25-octies del D.Lgs. 231/2001, che richiama i seguenti articoli del codice penale:

- **Ricettazione (art. 648 c.p.)** – Tale ipotesi di reato si configura nel caso in cui taluno acquisti o riceva o occulti denaro o cose provenienti da un qualsiasi delitto al fine di procurare a sé o ad altri un profitto. Ad esempio, qualora il dirigente della società incaricato di selezionare i fornitori e acquistare dell'hardware per CSI, acquisti tali beni sotto costo perché proveniente da un illecito (ad es. furto), con profitto per CSI.
- **Riciclaggio (art. 648 bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui taluno sostituisca o trasferisca denaro o beni provenienti da delitto ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa; ad esempio, qualora il dirigente di CSI versi quale corrispettivo per un Consulente somme di denaro che sa provenire da un delitto commesso da un cliente, al fine di occultare tale provenienza.
- **Impiego di denaro, beni o utilità di provenienza illecita (648-ter c.p.)** – Tale ipotesi di reato si configura nel caso in cui taluno impieghi in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto; ad esempio, qualora un dirigente della società utilizzi per attività pubblicitarie di CSI somme di denaro ricevute da un cliente, sapendo che tali somme provengono da delitto.

L'art. 64, comma 1, lett. f) abroga i commi 5 e 6 dell'art. 10 della l. n. 146/2006, di contrasto al crimine organizzato transnazionale, con la conseguenza che la commissione dei reati di cui agli artt. 648, 648 bis e 648 ter del c.p., diventa causa di responsabilità ex D.Lgs. n. 231/2001 anche nei casi in cui tali reati non si configurino come transnazionali.

Tali reati pertanto rientrano nella categoria dei reati di riciclaggio e non più in quella dei reati transnazionali.

La L. n. 186/2014, in vigore dal 1° gennaio 2015, ha inserito all'art. 25-octies D.Lgs. 231/2001 il reato di autoriciclaggio, punito dall'art. 648-ter.1 c.p.:

- **Autoriciclaggio (art. 648-ter.1 c.p.)** - Tale ipotesi di reato si configura nei confronti di chiunque, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

La persona fisica che commette un reato di riciclaggio è punita con la reclusione da un minimo di due ad un massimo di dodici anni e con una multa da 516,46 Euro fino a 25.000 Euro.

Per la Società sono previste sanzioni pecuniarie da 200 a 1000 quote (da 51,6 mila Euro a 1.549 mila Euro) e sanzioni interdittive per un periodo non inferiore a due anni.

In data 30 novembre 2021, è stato pubblicato in Gazzetta Ufficiale n. 285, Suppl. ord. n. 41, il Decreto legislativo n. 195 del 5 novembre 2021 di attuazione della VI Direttiva Antiriciclaggio (direttiva UE 2018/1673 del 23 ottobre 2018, sulla lotta al riciclaggio mediante diritto penale). La direttiva, oltre ad ampliare gli strumenti di contrasto al riciclaggio dei proventi illeciti, estende l'applicazione dei reati di ricettazione, riciclaggio, auto riciclaggio e reimpiego a tutti i proventi, frutto di reato, compresi i delitti colposi e le contravvenzioni. Il provvedimento entra in vigore il 15 dicembre 2021. Il decreto introduce modifiche alla fattispecie di ricettazione (art. 648 c.p.), riciclaggio (art. 648 bis c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.), autoriciclaggio (art. 648 ter.1 c.p.).

Per tutte tali fattispecie sono previsti (i.) l'ampliamento del catalogo dei reati presupposto, che ora comprende anche i delitti colposi e le contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi; (ii.) una diversa risposta sanzionatoria a seconda che il reato presupposto consista in un delitto o in una contravvenzione.

Per quanto riguarda la ricettazione sono inoltre previsti (i.) una aggravante, qualora il fatto sia stato commesso nell'esercizio di una attività professionale; (ii.) una nuova ipotesi di ricettazione di speciale tenuità, qualora il reato presupposto sia costituito da una qualsiasi contravvenzione.

Per il solo autoriciclaggio, la attenuante ad effetto speciale di cui al secondo comma, che in precedenza prevedeva la più mite sanzione della reclusione da uno a quattro anni, è ora qualificata come circostanza attenuante comune.

E' stata eliminata la condizione di procedibilità della richiesta del Ministro della giustizia prevista dall'articolo 9 c.p. per i reati di ricettazione e autoriciclaggio commessi dal cittadino all'estero.

Inoltre, l'art. 2 del D.Lgs 231/07 precisa che il riciclaggio è considerato tale anche se le attività, che hanno generato i beni da riciclare, si siano svolte nel territorio di un altro Stato comunitario o di un Paese terzo.

9.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Stipula e gestione dei rapporti contrattuali con clienti e controparti;**
- **Gestione approvvigionamenti, incarichi professionali e consulenze;**
- **Selezione e Amministrazione del Personale;**
- **Gestione Adempimenti Fiscali**

9.3 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo

Si riporta di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo. Tali principi si completano con la normativa aziendale di dettaglio che regola l'attività medesima.

Il provvedimento della Banca d'Italia del 26 marzo 2019 recante *“Disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria ai fini di riciclaggio e di finanziamento del terrorismo”* dispone che i destinatari della normativa implementino una specifica funzione antiriciclaggio indipendente e dotata di risorse adeguate, specificando i compiti che dovranno essere svolti da tale funzione.

La funzione può essere costituita in modo autonomo oppure nell'ambito di strutture organizzative diverse, quali la Compliance, o il Risk Management (è esclusa l'assegnazione alla funzione di revisione interna) oppure può essere esternalizzata, purchè il processo di gestione dei rischi sia ricondotto ad unità mediante la nomina di un Responsabile con compiti di coordinamento e di supervisione. In caso di esternalizzazione, la responsabilità rimane comunque in capo al destinatario.

Alla funzione sono assegnati compiti specifici quali:

- identificare le norme applicabili e valutare il loro impatto sui processi e le procedure interne;
- collaborare alla definizione del sistema dei controlli interni e delle procedure finalizzati alla prevenzione e al contrasto dei rischi di riciclaggio;
- verificare nel continuo l'adeguatezza del processo di gestione dei rischi di riciclaggio e
- l'idoneità del sistema dei controlli interni e delle procedure e proporre le modifiche organizzative e procedurali volte ad assicurare un adeguato presidio dei rischi di riciclaggio;
- condurre, in raccordo con il responsabile delle SOS, verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela;
- collaborare alla definizione delle politiche di governo del rischio di riciclaggio e delle varie fasi in cui si articola il processo di gestione di tale rischio;
- condurre, in raccordo con le altre funzioni aziendali interessate, l'esercizio annuale di autovalutazione dei rischi di riciclaggio a cui è esposto il destinatario;
- prestare supporto e assistenza agli organi aziendali e all'alta direzione;

- valutare in via preventiva il rischio di riciclaggio connesso all'offerta di prodotti e servizi nuovi;
- verificare l'affidabilità del sistema informativo per l'adempimento degli obblighi di adeguata verifica della clientela, conservazione dei dati e segnalazione delle operazioni sospette;
- trasmettere mensilmente alla UIF i dati aggregati concernenti l'operatività complessiva del destinatario;
- trasmettere alla UIF, sulla base delle istruzioni dalla stessa emanate, le comunicazioni oggettive concernenti operazioni a rischio di riciclaggio;
- curare, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di un adeguato piano di formazione, finalizzato a conseguire un aggiornamento su base continuativa del personale;
- informare tempestivamente gli organi aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti;
- predisporre flussi informativi diretti agli organi aziendali e all'alta direzione.

Il *Responsabile della funzione antiriciclaggio* si colloca tra i responsabili di funzioni aziendali di controllo e che deve essere in possesso di requisiti di indipendenza, autorevolezza e professionalità.

In particolare, la normativa prevede che il Responsabile non debba avere responsabilità dirette di aree operative o essere gerarchicamente dipendente da soggetti responsabili di tali aree.

E' richiesta anche la nomina della figura di Responsabile o, in sua vece, di Delegato alla segnalazione delle operazioni sospette, il cui nominativo va comunicato all'UIF. La delega può essere attribuita al Responsabile antiriciclaggio, ma non oggetto di esternalizzazione.

In particolare, con riferimento alle aree a rischio devono essere adottate, le seguenti procedure e regole di condotta:

- devono essere rispettate Policy e Procedure adottate in ottemperanza al D.Lgs. 231/2007 in materia di antiriciclaggio, e quelle poste in essere in base alle "Istruzioni operative per l'individuazione di operazioni sospette" della Banca d'Italia;
- in particolare, si devono tenere dei comportamenti conformi alle prescrizioni contenute nella Policy e nel Manuale Antiriciclaggio che illustra a tutto il personale della SGR le principali regole dettate dalla normativa antiriciclaggio italiana.

9.4 Procedure specifiche

Ad integrazione delle procedure e regole di condotta sopra delineate, devono essere rispettate le seguenti procedure descritte per le singole aree a rischio.

9.4.1 Stipula e gestione rapporti contrattuali con la clientela e le controparti

In linea generale gli aspetti caratterizzanti della Policy e del Manuale Operativo in materia di antiriciclaggio vigenti possono essere riconducibili ai seguenti elementi:

1. identificazione di ogni cliente, incluso l'eventuale titolare effettivo;

2. indicazione del “quando” (es. instaurazione di un rapporto continuativo, esecuzione di un’operazione occasionale di importo superiore alle soglie stabilite per legge, ecc.) e del “come” (es. modalità di identificazione del cliente, del titolare effettivo, di scopo e natura delle transazioni, ecc.) adempiere a tali obblighi;
3. definizione di un approccio basato sul rischio, per cui gli obblighi di adeguata verifica della clientela si articolano in differenti gradi di *due diligence* commisurati al profilo di rischio del cliente (es. obblighi semplificati per Intermediari Finanziari e per Uffici della Pubblica Amministrazione, e obblighi rafforzati per clienti non fisicamente presenti all’instaurazione del rapporto, per soggetti politicamente esposti – PEP³ – non residenti, per enti corrispondenti extracomunitari, per clientela con profilo di rischio riciclaggio massimo, ecc.);
4. monitoraggio dell’attività svolta da ogni cliente, in particolare:
 - monitoraggio nel medio-lungo periodo da parte Strutture organizzative preposte che garantisca un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l’area geografica di riferimento (con particolare riguardo all’operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell’operazione, 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 Strutture preposte al controllo interno della puntuale esecuzione nel pieno rispetto dei termini e delle disposizioni di legge e della normativa interna, delle attività delle Strutture operative;
 - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
 - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell’utilizzo del contante e dei titoli al portatore;
 - registrazione dei rapporti e delle operazioni nell’ Archivio Unico Informatico (AUI) e conservazione dei documenti e delle informazioni, secondo quanto stabilito dall’Allegato tecnico di UIF
5. identificazione e comunicazione di comportamenti sospetti o inconsueti che possano nascondere attività di riciclaggio tutti i rapporti continuativi e le operazioni che comportano la trasmissione di mezzi di pagamento devono essere processati con modalità che consentano la registrazione procedurale nell’archivio standardizzato con dati corretti e completi, anche avvalendosi di controlli automatici sulla qualità dei dati. Un archivio ordinato consente, infatti, tra l’altro, di evadere prontamente le richieste di informazioni da parte delle competenti Autorità e di ricostruire l’operatività della clientela anche a fini di monitoraggio e della corretta definizione del profilo di rischio: a tale fine è indispensabile procedere alle attività di “integrazione” e “sistemazione” delle operazioni o dei rapporti in stato di “sospeso” entro i termini consentiti dalle procedure e comunque nei termini previsti dalla norma;
6. obbligo di astensione dall’apertura di un nuovo rapporto o dal mantenimento di un rapporto in essere nel caso in cui l’operatore non sia in grado di adempiere correttamente agli obblighi di

³ L’acronimo PEP sta per Politically Exposed Person o, in italiano, Persona Politicamente Esposta. Per la definizione di PEP fare riferimento all’art. 1, comma 2 lettera o) del D. Lgs. n. 231/2007 e all’art. 1 dell’Allegato Tecnico al D. Lgs. n.231/2007.

adeguata verifica o sussista il sospetto che vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;

7. obbligo di segnalazione delle operazioni sospette secondo gli indicatori di anomalia che devono essere oggetto di costante formazione del personale addetto e l'obbligo di comunicazione delle infrazioni alle disposizioni in tema di limitazioni per l'utilizzo del contante e dei titoli al portatore;
8. l'obbligo di registrazione nell'Archivio Unico Informatico (AUI) o in altro archivio standardizzato dei rapporti, dei dati identificativi e delle operazioni poste in essere dalla clientela;
9. monitoraggio di tutte le transazioni realizzate con Paesi che minacciano la pace e la sicurezza internazionale (Paesi inseriti nelle *sanction list*⁴);
10. adozione di adeguate misure di formazione del personale per garantire il corretto recepimento delle disposizioni normative e la loro corretta applicazione;
11. possibilità di assicurare la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate (in particolare l'Unità Organizzativa di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo);
12. riservatezza delle informazioni, con particolare riguardo a quelle relative all'individuazione dei titolari effettivi, alla profilatura dei clienti ed ai processi di monitoraggio delle operazioni e di segnalazione delle operazioni sospette, mediante l'adozione di idonee misure informatiche e fisiche;

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;
- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione.

⁴Al fine di prevenire l'insorgere di potenziali minacce, i Governi e le Organizzazioni Internazionali stilano specifiche liste – *sanction list* – di determinati Paesi, soggetti ed entità le cui attività divengono soggette a controllo e monitoraggio da parte delle Istituzioni Finanziarie. Tali liste sono definite ed aggiornate da Istituzioni quali le Nazioni Unite (NU), l'Unione Europea (UE), le banche centrali e, per gli Stati Uniti, l'Office of Foreign Assets Control (OFAC).

La SGR, coerentemente all'approccio basato sul rischio riciclaggio raccomandato dalla Banca d'Italia, prevede lo svolgimento di specifici controlli antiriciclaggio estesi anche sulle controparti oggetto di investimento (aziende target dei Fondi Gestiti).

L'attività di controllo sulle controparti, pur non costituendo un vero e proprio processo di adeguata verifica, rappresenta un presidio idoneo a gestire eventuali rischi reputazionali in capo alla SGR e a individuare l'eventuale presenza di pregiudizievoli in capo alle controparti. Le verifiche in ordine alla controparte d'investimento ed alla struttura societaria dell'operazione sono approfondite mediante l'autonoma acquisizione di documenti pubblici (es. visure camerali) e la consultazione di banche dati specializzate, al fine di identificare i legali rappresentanti delle controparti, i relativi poteri di firma e la destinazione e/o provenienza dei fondi a regolamento dei corrispettivi.

9.4.2 Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze

La procedura di gestione fornitori, acquisto di beni e servizi della SGR prevede:

- selezione dei fornitori e partner commerciali secondo criteri omogenei e predeterminati; tracciabilità del processo di raccolta informazioni e archiviazione;
- un adeguato processo di identificazione, approvazione e registrazione dei fornitori, consulenti e terze parti, che preveda la verifica dell'attendibilità commerciale e professionale e la verifica periodica della correttezza ed aggiornamento delle informazioni acquisite;
- verifica della regolarità dei pagamenti, anche con riferimento alla coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione.

Si confrontino, inoltre, le procedure specifiche previste per il processo "*Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze*" nella Parte Speciale – *REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI*".

9.4.3 Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi

Il processo di selezione del personale e dei collaboratori e degli agenti prevede:

- l'adozione di procedure di selezione ed assunzione trasparenti ed omogenee, garantendo la completa tracciabilità del processo e dei criteri di selezione;
- l'esecuzione della verifica, nel pieno rispetto della normativa in materia di tutela dei dati personali, dei dati e delle informazioni raccolte in fase di selezione dai candidati.

Si confrontino, inoltre, le procedure specifiche previste per il processo "*Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi*" – *REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI*".

9.4.4 Gestione degli aspetti fiscali

Si rimanda alle Parti Speciali “REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL’UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL’AUTORITÀ GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI” e “REATI SOCIETARI” ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

9.5 Controlli dell’Organismo di Vigilanza

L’Organismo di Vigilanza svolge controlli periodici sulle attività potenzialmente a rischio di commissione dei reati di riciclaggio, tra cui:

- verifica l’esistenza di un adeguato processo per la definizione e invio dei flussi informativi a proprio favore;
- richiede, eventualmente in via periodica, le informazioni rilevanti ai fini dell’esercizio delle proprie funzioni di vigilanza;
- verifica che l’operatività della SGR sia svolta nel rispetto delle policy e procedure interne relativamente alla prevenzione del riciclaggio e del finanziamento del terrorismo;
- verifica l’adeguatezza delle procedure di identificazione della clientela
- verifica l’adeguatezza dei presidi di prevenzione e controllo adottati in relazione alla situazione di rischio per comprendere e valutare il rischio di riciclaggio dei propri clienti;
- verifica la predisposizione dei piani formativi e la loro esecuzione ai fini di formare i dipendenti relativamente ai rischi di commissione dei reati previsti dal D.Lgs. n. 231/2007 ed ai relativi obblighi di segnalazione di operazioni sospette all’Organismo di Vigilanza;
- verifica l’adeguatezza delle procedure e delle modalità di gestione delle segnalazioni di operazioni sospette ricevute da qualsiasi fonte, interna o esterna alla SGR.

10. REATI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL’AUTORITÀ GIUDIZIARIA

10.1 La fattispecie di reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria

L’art. 25 decies del D.Lgs. 231/01 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria richiama i seguenti articoli del codice penale:

- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria (art. 377 bis c.p.)** – Reato commesso dal soggetto che, 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 la persona chiamata a rendere davanti l’autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

In relazione alla commissione del delitto di cui all’art. 377-bis del codice penale, si applica all’ente la sanzione pecuniaria fino a cinquecento quote (da 129 mila Euro a 775 mila Euro).

10.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- Gestione del contenzioso giudiziale e stragiudiziale.

10.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione gestione e controllo:

È previsto l'espresso divieto a carico dei responsabili di funzione, dei dipendenti e dei collaboratori esterni di GRADIENTE di:

- adottare comportamenti che violino i principi e le procedure aziendali previste dalla presente Parte Speciale;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle disciplinate all'art. 377 bis del codice penale;

La presente Parte Speciale prevede, conseguentemente, l'espresso divieto a carico dei Destinatari di agire al fine di influenzare il comportamento di soggetti chiamati a rendere dichiarazioni di fronte l'autorità giudiziaria.

10.4 Procedure specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi.

10.4.1 Gestione del contenzioso giudiziale

In aggiunta alle disposizioni previste nella Parte Speciale *"REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI"*, in particolare ove concernenti la gestione del contenzioso giudiziale, sono adottate le seguenti disposizioni in capo ai Destinatari:

- adottare comportamenti improntati alla massima correttezza ed etica, nel pieno rispetto dei principi sanciti dal Codice Interno di Comportamento e dalle procedure interne nei rapporti con studi legali esterni o consulenti incaricati di assistere la SGR nella gestione di contenziosi;
- operare esclusivamente nell'ambito dell'incarico ricevuto, delle deleghe e poteri conferiti in merito all'avvio di contenzioni contrattuali, con dipendenti o attinenti l'area dei rapporti di lavoro, fiscali o di ogni altro genere;
- in relazione alle spese legali, di consulenza o inerenti accordi transattivi:
 - a. adottare adeguati processi di gestione delle risorse finanziarie;
 - b. assicurare la tracciabilità dei flussi di pagamento;
 - c. verificare le motivazioni sottostanti ad eventuali scostamenti dal budget.

- segnalare immediatamente all'Organismo di Vigilanza ogni comportamento anomalo o contrario al Codice Interno di Comportamento o alle regole e principi di comportamento stabiliti nella presente Parte Speciale.

10.5 Controlli dell'Organismo di Vigilanza

Per la descrizione dei controlli suggeriti per specifici processi, si rimanda a quanto riportato nella Parte Speciale *“REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI”*.

11. REATI AMBIENTALI

11.1 Le fattispecie di reato

L'art. 25-undecies del Decreto disciplina i reati ambientali e, precisamente, individua gli illeciti dai quali, nella materia della tutela penale dell'ambiente, fondata su disposizioni di matrice comunitaria, discende la responsabilità amministrativa degli enti. L'art. 25-undecies del D.Lgs. n. 231/01, in vigore dal 16 agosto 2011, nel testo dapprima inserito dal D.Lgs. n. 121/11, emanato in recepimento delle Direttive 2008/99/CE e 2009/123/CE, e successivamente modificato dalla L. n. 68/15, in vigore dal 29 maggio 2015, che ha introdotto nel codice penale i nuovi delitti contro l'ambiente.

- **Inquinamento ambientale (art. 452-bis c.p.)** - La norma punisce chi cagiona abusivamente una compromissione o un deterioramento significativi e misurabili delle acque, dell'aria, del suolo o del sottosuolo, di un ecosistema o della biodiversità.
- **Disastro ambientale (art. 452-quater c.p.)** - La norma punisce chi abusivamente provoca un disastro ambientale, che consiste nell'alterazione dell'equilibrio di un ecosistema che sia irreversibile, o la cui eliminazione sia particolarmente onerosa ed eccezionale, oppure nell'offesa all'incolumità pubblica, in ragione della gravità del fatto, per estensione, o per gli effetti, o per il numero di persone offese o esposte a pericolo.
- **Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)** - Sono punite molteplici condotte abusive (cessione, acquisto, ricezione, trasporto, importazione, esportazione, detenzione, abbandono, ecc.) concernenti materiali ad alta radioattività.
- **Associazione a delinquere con aggravante ambientale (art. 452-octies c.p.)** - La norma prevede una specifica aggravante di pena per i reati di associazione a delinquere aventi lo scopo di commettere taluno dei delitti ambientali previsti dal codice penale. Se si tratta di reato di *“Associazione mafiosa”*, costituisce aggravante il fatto stesso dell'acquisizione della gestione o del controllo di attività economiche, di concessioni, autorizzazioni, appalti o di servizi pubblici in materia ambientale.
- **Reati concernenti specie animali o vegetali selvatiche protette o habitat protetti (artt. 727-bis e 733-bis codice penale.)** - Sono punite le condotte di prelievo, possesso, uccisione o distruzione di esemplari appartenenti a specie animali o vegetali selvatiche protette, fuori dei casi consentiti dalla legge e salvo che si tratti di danni considerati trascurabili, per quantità di esemplari o per impatto sullo stato di conservazione della specie. È altresì punita la condotta di distruzione o di deterioramento tale da compromettere lo stato di conservazione di un habitat situato all'interno di un

sito protetto. Le norme comunitarie elencano le specie animali o vegetali protette e individuano le caratteristiche che impongono la classificazione da parte della legge nazionale di un habitat naturale o di specie come zona a tutela speciale o zona speciale di conservazione.

- **Violazioni della disciplina degli scarichi (art. 137, commi 2, 3, 5, 11 e 13, C.A.)** - L'art. 137 C.A. punisce una serie di violazioni della disciplina degli scarichi ed in particolare: gli scarichi senza autorizzazione di acque reflue industriali contenenti determinate sostanze pericolose, oppure in difformità delle prescrizioni dell'autorizzazione o nonostante la sua sospensione o revoca, nonché gli scarichi di sostanze pericolose oltre i valori limite; le violazioni dei divieti di scarico sul suolo, nelle acque sotterranee e nel sottosuolo fuori dalle ipotesi ammesse dagli artt. 103 e 104 C.A. Infine, sono sanzionate le violazioni dei divieti di scarichi in mare effettuati da navi o aerei di sostanze pericolose previste dalle convenzioni internazionali, salvo che si tratti di scarichi autorizzati di quantità rapidamente biodegradabili.
- **Violazioni della disciplina sulla gestione dei rifiuti (art. 256, commi 1, 3, 5 e comma 6, 1° periodo, C.A.)** - Le condotte punite consistono nella raccolta, trasporto, recupero, smaltimento commercio o intermediazione di rifiuti senza le prescritte autorizzazioni, iscrizioni all'Albo nazionale gestori ambientali e comunicazioni alle competenti autorità, oppure in difformità delle disposizioni contenute nelle autorizzazioni o impartite dalle autorità o in carenza dei requisiti prescritti. Sono altresì punite le attività di realizzazione o gestione di una discarica non autorizzata, di miscelazione di rifiuti pericolosi di diverso genere tra di loro o con rifiuti non pericolosi e di deposito di rifiuti sanitari pericolosi presso il luogo di produzione, per quantitativi superiori a 200 litri o equivalenti.
- **Omissione di bonifica per i casi di inquinamento del suolo, del sottosuolo, delle acque superficiali o sotterranee (art. 257, commi 1 e 2, C.A.)** - Salvo che il fatto non costituisca più grave reato (ad es. quello di cui sopra all'art. 452-bis c.p.) è punito chi avendo cagionato l'inquinamento in oggetto con il superamento delle concentrazioni soglia di rischio non provvede alle dovute comunicazioni alle competenti autorità e alla bonifica del sito ai sensi dell'art. 242 C.A. L'effettuazione della bonifica costituisce condizione di non punibilità anche per le contravvenzioni ambientali previste da altre leggi speciali per il medesimo evento.
- **Falso in certificato di analisi rifiuti (art. 258, comma 4, 2° periodo, C. A.)** - Commette il delitto in questione chi fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti riportate in un certificato di analisi dei rifiuti e chi utilizza il certificato falso per il trasporto dei rifiuti.
- **Traffico illecito di rifiuti (art. 259, comma 1, C. A.)** - La norma punisce chi effettua una spedizione di rifiuti transfrontaliera in violazione del Regolamento CE n. 259/93, che peraltro è stato abrogato e sostituito dal Regolamento CE n. 1013/2006.
- **Attività organizzate per il traffico illecito di rifiuti (art. 452 – quaterdecies, commi 1 e 2 c.p.)** - Tale delitto è commesso da chi, al fine di conseguire un ingiusto profitto, cede, riceve, trasporta, esporta, importa o comunque gestisce abusivamente ingenti quantitativi di rifiuti. Deve trattarsi di fatti non episodici, ma di attività continuative, per lo svolgimento delle quali siano stati predisposti appositi mezzi ed organizzazione. È prevista un'aggravante di pena per il caso di rifiuti altamente radioattivi.
- **Falsità nella tracciabilità dei rifiuti mediante il SISTRI (art. 260-bis, comma 6 – comma 7, 2° e 3° periodo - comma 8, C. A.)** - Al sistema informatico di controllo della tracciabilità dei rifiuti,

denominato SISTRI, partecipano obbligatoriamente o su base volontaria, secondo i criteri di cui all'art. 188-ter C.A., i produttori di rifiuti e gli altri soggetti che intervengono nella loro gestione (commercianti, intermediari, consorzi di recupero o riciclaggio, soggetti che compiono operazioni di recupero o di smaltimento, trasportatori). In tale contesto sono puniti i delitti consistenti nel fornire false indicazioni sulla natura e sulle caratteristiche di rifiuti al fine della predisposizione di un certificato di analisi dei rifiuti da inserire in SISTRI, nell'inserire nel sistema un certificato falso o nell'utilizzare tale certificato per il trasporto dei rifiuti. È altresì punito il trasportatore che accompagna il trasporto con una copia cartacea fraudolentemente alterata della scheda SISTRI compilata per la movimentazione dei rifiuti.

- **Violazioni della disciplina delle emissioni in atmosfera (art. 279, comma 5, C. A.)** - La norma punisce le emissioni in atmosfera compiute nell'esercizio di uno stabilimento, superiori ai valori limite stabiliti dalla legge o fissati nelle autorizzazioni o prescrizioni delle competenti autorità, quando siano superati anche i valori limite di qualità dell'aria previsti dalla vigente normativa.
- **Violazioni in tema di commercio e detenzione di animali o vegetali in via di estinzione o di mammiferi e rettili pericolosi (L. n. 150/1992, art. 1, commi 1 e 2 – art. 2, commi 1 e 2 – art. 3-bis, comma 1 - art. 6, comma 4)** - Gli illeciti consistono nell'importazione, esportazione, trasporto, detenzione di esemplari di animali o di vegetali in violazione delle disposizioni comunitarie e internazionali che impongono particolari autorizzazioni, licenze e certificazioni doganali, e nella falsificazione o alterazione dei predetti documenti. È vietata altresì la detenzione di determinati mammiferi e rettili pericolosi.
- **Sostanze lesive dell'ozono stratosferico (L. n. 549/1993, art. 3, comma 6)** - La legge vieta il commercio, l'utilizzo, l'importazione, l'esportazione, la detenzione di sostanze lesive dell'ozono atmosferico dalla stessa elencate.
- **Inquinamento provocato dalle navi (D.Lgs. n. 202/2007, artt. 8 e 9)** - La norma sanziona i comandanti delle navi, i membri dell'equipaggio, i proprietari e gli armatori che dolosamente o colposamente sversano in mare idrocarburi o sostanze liquide nocive trasportate alla rinfusa, fatte salve le deroghe previste.

11.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze**
- **Gestione dei rischi in materia ambientale;**

11.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo.

I Destinatari sono tenuti, nei rispettivi ambiti, a:

- vigilare, per quanto di competenza, sul rispetto degli adempimenti in materia ambientale, in particolare sull'osservanza delle norme operative sul raggruppamento e deposito temporaneo dei rifiuti secondo la loro classificazione;
- segnalare tempestivamente eventuali situazioni di pericolo per l'ambiente e violazioni alle regole di comportamento e alle procedure aziendali in materia;

- effettuare la raccolta dei rifiuti assimilabili agli urbani, urbani e speciali in conformità alle normative e alle prassi di buona tecnica e di prevenzione ambientale (ad esempio, per la raccolta delle cartucce e toner esauriti, occorre utilizzare la confezione originale e depositare le confezioni contenenti il materiale da smaltire negli appositi contenitori);
- affidare i rifiuti speciali, pericolosi e non pericolosi a società di trasporto e recupero e smaltimento autorizzate ed iscritte ai relativi Albi, avendo cura di accertare il conseguimento, anche da parte di fornitori e consulenti, delle prescritte autorizzazioni, iscrizioni o comunicazioni;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es.: A.S.L., Vigili del Fuoco, ARPA, Comune, Provincia, ecc.) in occasione di accertamenti/procedimenti ispettivi; osservare le disposizioni di legge impartite dalle Autorità competenti;
- rispettare la policy di sostenibilità che stabilisce, tra l'altro, regole comportamentali per la tutela dell'ambiente; segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, qualsiasi eventuale situazione di emergenza ambientale connessa all'attività.

È fatto inoltre divieto di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- depositare i rifiuti al di fuori delle aree appositamente adibite e consegnare i rifiuti speciali così come definiti dalla vigente normativa interna a fornitori incaricati del trasporto che non siano autorizzati alla gestione dei rifiuti;
- in sede di realizzazione delle prescritte misure di controllo, perseguire l'obiettivo di risparmio costi e tempi a scapito della tutela dell'ambiente;
- in sede di ispezioni e verifiche, adottare comportamenti finalizzati ad influenzare indebitamente, nell'interesse della SGR, il giudizio/parere delle Autorità pubbliche di controllo;
- porre in essere o dare causa a violazioni della regolamentazione in materia di gestione ambientale;

I Destinatari sono inoltre tenuti a osservare le previsioni legislative esistenti in materia e i principi contenuti nel Codice Interno di Comportamento. Il Personale della SGR, a qualsiasi titolo coinvolto nelle attività a rischio-reato identificate, è inoltre tenuto a rispettare le disposizioni ed eseguire i controlli di competenza formalizzati nella normativa interna di volta in volta rilevante e nell'ulteriore documentazione adottata in attuazione del sistema dei controlli e dei principi di comportamento contenuti nella presente Parte Speciale.

11.4 Procedure specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi.

11.4.1 Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze

La scelta e qualifica dei fornitori che si occupano delle operazioni di recupero e smaltimento dei rifiuti, prevede la verifica circa il possesso delle qualificazioni/ autorizzazioni/abilitazioni/certificazioni richieste ai sensi della normativa per l'esercizio dell'attività, che ne dà conto nell'ambito delle riunioni periodiche con la SGR.

E' previsto un controllo sul corretto espletamento, da parte dei fornitori, dei servizi di manutenzione/pulizia (servizi agli edifici, servizi alle persone, ecc.) degli immobili.

11.4.2 Gestione dei rischi ambientali

La SGR adotta una specifica procedura aziendale denominata **Sistema di Gestione Ambientale e Sociale (ESG)** finalizzata alla corretta gestione di tematiche ambientali e sociali. La SGR mediante l'applicazione di tale procedura intende uniformarsi alla normativa nazionale e comunitaria in materia ambientale e sociale, perseguire un miglioramento continuo in tale ambito e garantire la conformità ai requisiti sociali ed ambientali delle partecipate dai FIA gestiti. La SGR garantisce, mediante l'applicazione della procedura, che vengano eseguite le adeguate valutazioni e che vengano individuati i rischi, gli impatti e l'adozione di misure di prevenzione.

La SGR considera la sostenibilità come un valore aggiunto per la corretta gestione dei FIA. L'adozione di un approccio di gestione sostenibile contribuisce ad una significativa riduzione dei rischi, siano essi reputazionali o legati alla corretta gestione delle opportunità di business e permette una visione delle performance allargata poiché comprende anche i risultati sociali e ambientali.

Di seguito sono riportate alcune importanti linee guida aziendali in ambito ambientale.

Environmental

Gradiente ha molto a cuore il rispetto ambientale e la lotta alla riduzione dell'inquinamento e dello spreco:

- tutto lo staff è impegnato nell'adempiere al proprio dovere di riciclaggio dei rifiuti, come previsto dal piano della nostra città; sono quindi presenti in ufficio contenitori per la raccolta differenziata;
- gli impianti dei sistemi di riscaldamento/raffreddamento nei nostri uffici sono sotto-posti a manutenzione programmata annuale per garantire un funzionamento corretto ed efficiente al fine di risparmiare energia e limitare gli sprechi;
- l'impianto di illuminazione e le luci nell'edificio sono per la maggior parte in tecnologia led, efficienti dal punto di vista energetico;
- le impostazioni di stampa sono impostate automaticamente per la stampa fronte / retro ed è adottato l'uso di carta riciclata per i documenti ad uso interno;
- lo staff di GRADIENTE utilizza principalmente il treno per i viaggi interni ed ove possibile preferisce l'uso dell'auto elettrica.

11.5 Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha facoltà discrezionale di porre in essere le attività di controllo periodico sulle attività aziendali potenzialmente a rischio di commissione dei reati ambientali. Tali controlli sono volti a verificare la corretta esplicazione delle regole definite nel Modello e, in particolare, delle procedure interne in essere.

12. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE

12.1 La fattispecie di reato

L'articolo 2 del D.lgs. 16 luglio 2012, n. 109 (recante "Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare") ha introdotto nel Decreto l'articolo 25-

duodecies, rubricato “Impiego di cittadini di paesi terzi il cui soggiorno è irregolare” prevedendo la responsabilità amministrativa degli enti per il reato previsto dall’art. 22, comma 12-bis del D.lgs. n. 286/1998 (Testo Unico delle disposizioni concernenti la disciplina dell’immigrazione e norme sulle condizioni dello straniero).

Di seguito si indica la fattispecie penale richiamata dall’art. 25 *duodecies* del Decreto.

Articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286

12. Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000,00 euro per ogni lavoratore impiegato.

12-bis. Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

- a) se i lavoratori occupati sono in numero superiore a tre;
- b) se i lavoratori occupati sono minori in età non lavorativa;
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell’articolo 603-bis del codice penale (NDR: ovvero a “situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro”).

12.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione del processo di selezione, assunzione, amministrazione del personale e del sistema degli incentivi.**

12.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi del Reato descritto al precedente Paragrafo 11.1.

In particolare, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla gestione dei rapporti con controparti assunzione e gestione delle risorse umane;
- rispettare la normativa vigente e i principi del Codice Interno di Comportamento cui attenersi al fine di non violare le prescrizioni anche procedurali previste dalla normativa sull’immigrazione;
- verificare, per il tramite di pareri legali o di altri professionisti, l’eventualità che una condotta della SGR possa configurare un reato previsto dal Testo Unico Immigrazione.
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuto o sospettato lo svolgimento di attività illecite con riferimento alle fattispecie penali punite dal “Testo

Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero" (di seguito "Testo Unico Immigrazione") e, in generale, dalla normativa sulla immigrazione.

12.4 Procedure Specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio

12.4.1 Gestione del processo di selezione, assunzione, amministrazione del personale

In caso di assunzione di cittadini di paesi terzi già in possesso del permesso di soggiorno, la SGR verifica l'esistenza e validità di quest'ultimo, unitamente all'ulteriore documentazione utile per perfezionare l'assunzione.

In caso di assunzione di cittadini di paesi terzi non in possesso del permesso di soggiorno, la SGR dovrà provvedere direttamente o a mezzo consulente del lavoro:

- a) alla richiesta nominativa di nulla osta (autorizzazione all'assunzione) da presentare presso l'ufficio della Prefettura competente territorialmente;
- b) a consegnare il nulla osta, una volta rilasciato, al cittadino che si intende assumere, affinché lo stesso possa richiedere ai competenti uffici il rilascio del visto di ingresso per motivi di lavoro subordinato e quindi, a seguito dell'ingresso in Italia, il permesso di soggiorno;
- c) a farsi consegnare il permesso di soggiorno o la copia della domanda di rilascio del permesso di soggiorno presentata all'ufficio postale e la relativa ricevuta;
- d) ad archiviare copia della documentazione di cui al punto c) che precede unitamente al contratto di soggiorno e lavoro;
- e) a provvedere alle comunicazioni previste per legge al Centro per l'impiego e agli altri Enti competenti, assicurando che le informazioni trasmesse siano veritiere, complete e basate su idonea documentazione.

In caso di assunzione di personale straniero con permesso di soggiorno la SGR mantiene monitorate le scadenze dei permessi di soggiorno e degli eventuali rinnovi dei lavoratori di paesi terzi assunti alle dipendenze/distaccati anche a mezzo dei sistemi informatici ad hoc utilizzati dalla SGR.

Inoltre, la SGR:

- in prossimità della scadenza del permesso di soggiorno invia comunicazioni ai lavoratori di paesi terzi;
- in corso di rapporto di lavoro, verifica la presentazione, da parte del lavoratore straniero, della domanda di rinnovo del permesso di soggiorno (di cui il lavoratore deve esibire copia della ricevuta rilasciata dall'ufficio postale presso il quale è stata effettuata la domanda), in prossimità della scadenza della validità dello stesso e comunque non oltre sessanta giorni dalla stessa;
- in sede di assunzione viene previsto l'impegno del lavoratore assunto dalla SGR di trasmettere alla SGR stessa qualunque comunicazione, lettera e richiesta proveniente dalle Autorità e uffici

competenti (Questura, Prefettura, Centro per l'Impiego) in merito alla validità o scadenza del permesso di soggiorno;

- assicura una corretta informativa e/o formazione dei Destinatari coinvolti nel Processo a rischio sopraindicato circa la normativa a disciplina dell'assunzione di lavoratori di paesi terzi

Tutta la documentazione oggetto del presente Processo a rischio (atti, verbali, contratti, ricevute, permessi di soggiorno ed altri documenti), in formato sia elettronico che cartaceo, deve essere archiviata e facilmente rintracciabile; in particolare deve essere assicurata la tracciabilità delle fonti/elementi informativi e deve essere curata l'archiviazione di tutta la relativa documentazione prodotta/ricevuta con riferimento alle attività propedeutiche e conseguenti alla presentazione della domanda di nulla osta all'assunzione di lavoratore straniero.

12.5 Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha facoltà discrezionale di porre in essere le attività di controllo periodico sulle attività aziendali potenzialmente a rischio di commissione dei reati legati all'impiego di cittadini di paesi terzi. Tali controlli sono volti a verificare la corretta esplicazione delle regole definite nel Modello e, in particolare, delle procedure interne in essere.

A questo fine, l'Organismo di Vigilanza provvede a:

- valutare l'efficacia e monitorare il rispetto dei principi definiti nel presente Modello, nel Codice Interno di Comportamento e nelle Procedure Aziendali in materia di selezione e gestione di personale di paesi terzi.

13. REATI TRIBUTARI

13.1 Le fattispecie di reati tributati

Il D.lgs. n. 75/2020 inserisce alcuni ulteriori reati tributari nel D.lgs. 231, nel corpo dell'art. 25-*quinqüesdecies*, introdotto ad opera della legge n. 157/2019, che disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica in presenza della commissione di determinati reati tributari.

Di seguito si indicano le fattispecie di reato enucleate nell'art. 25 – *quinqüesdecies*:

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 comma 1 e comma 2 bis del D. Lgs. 10 marzo 2000 n. 74):**

(1) È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

(2) Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

(2-bis) Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Si evidenzia che, secondo la definizione prevista dall'art. 1 D. Lgs. n. 74/2000, "per fatture per operazioni inesistenti si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in

base alle norme tributarie, emessi a fronte di operazioni non realmente effettuate in tutto o in parte o che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero che riferiscono l'operazione a soggetti diversi da quelli effettivi".

• **Dichiarazione fraudolenta mediante altri artifici (art. 3 del D. Lgs. 10 marzo 2000 n. 74):**

(1) Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica 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, quando, congiuntamente:

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

(2) Il fatto si considera commesso 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.

(3) Ai fini dell'applicazione della disposizione del comma 1, 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.

Ai fini dell'applicazione delle suddette disposizioni, 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.

Entrambi i reati si perfezionano con la presentazione delle dichiarazioni. Sono però puniti anche i delitti tentati, ai sensi dell'art. 6 del D. Lgs. n. 74/2000, qualora siano compiuti atti preparatori della dichiarazione fraudolenta, che possano consistere ad esempio nella sola annotazione delle informazioni non veritiere nella contabilità, al fine di evadere l'IVA per un valore non inferiore a € 10 milioni e i fatti avvengano in parte in Italia e in parte in altro Stato UE.

• **Emissione di fatture o altri documenti inesistenti (art. 8 comma 1 e comma 2 bis del D. Lgs. 10 marzo 2000 n. 74):**

(1) È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

(2) Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di piu' fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

(2-bis) Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Ai fini dell'applicazione della disposizione sopra indicata, l'emissione o il rilascio di piu' fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

- **Occultamento e distruzione di documenti contabili** (art. 10 del D. Lgs. 10 marzo 2000 n.74):

(1) Salvo che il fatto costituisca piu' grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge 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.

- **Sottrazione fraudolenta al pagamento di imposte** (art. 11 del D. Lgs. 10 marzo 2000 n. 74):

(1) È punito con la reclusione da sei mesi a quattro anni chiunque, 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, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

(2) È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per se' o per altri un pagamento parziale dei tributi e relativi accessori, indica 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. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

- **Dichiarazione infedele** (art. 4 D. Lgs. n. 74/2000)
- **Omessa dichiarazione** (art. 5 D. Lgs. n.74/2000)
- **Indebita compensazione** (art. 10-quater D. Lgs. n. 74/2000)

Tali reati puniscono rispettivamente chi:

- nelle dichiarazioni annuali dei redditi o IVA indica elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti, e siano superate determinate soglie di rilevanza penale;
- non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte (o la dichiarazione di sostituto di imposta) quando è superata una determinata soglia di imposta evasa;
- non versa le imposte dovute utilizzando in compensazione crediti non spettanti, per un importo annuo superiore a una determinata soglia.

Dette condotte comportano anche la responsabilità amministrativa ai sensi del D. Lgs. n. 231/2001 solo se hanno ad oggetto l'evasione dell'IVA per un importo non inferiore a € 10 milioni e se sono commesse nell'ambito di sistemi fraudolenti transfrontalieri. In presenza di entrambe le circostanze il reato di dichiarazione infedele è punito, ai sensi dell'art. 6 del D. Lgs. n. 74/2000, anche se è solo tentato, quando cioè sussistano atti preparatori, quali ad esempio l'omissione di obblighi di fatturazione, che potranno quindi aver effetto sulla successiva dichiarazione, se tali fatti siano compiuti anche nel territorio di un altro Stato membro dell'UE.

13.2 Individuazione delle aree sensibili

Costituiscono situazioni di particolare attenzione per la SGR, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- **Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze;**
- **Gestione degli aspetti fiscali;**
- **Gestione dei rapporti con il Collegio Sindacale e la Società di Revisione.**

13.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo.

Il rischio di commissione dei reati in oggetto è potenzialmente presente in tutte le attività operative svolte dai dipendenti o da collaboratori riferite agli aspetti contabili, alla predisposizione degli adempimenti fiscali, alla gestione degli acquisti.

Al fine di evitare la commissione dei reati presupposto in analisi, è opportuno fare **divieto** di:

- effettuare qualsiasi tipo di pagamento nell'interesse di CSI in assenza di adeguata documentazione di supporto;
- effettuare pagamenti nei confronti di un beneficiario non coincidente con la controparte contrattuale;
- utilizzare strumenti anonimi per il compimento di azioni o di operazioni di trasferimento di importi rilevanti (es. contante o altro strumento finanziario al portatore);
- emettere fatture o rilasciare documenti per operazioni inesistenti, in tutto o in parte, al fine di consentire a terzi di commettere un'evasione fiscale;
- indicare elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti in tutto o in parte;
- effettuare registrazioni false, incomplete o ingannevoli ed istituire fondi occulti o non registrati;
- occultare e/o distruggere la documentazione contabile e fiscale di cui è obbligatoria la conservazione;
- utilizzare i fondi e le risorse di CSI senza formale autorizzazione;
- alienare simultaneamente eventuali beni di CSI per rendere inefficace le procedure di riscossione coattiva ai fini fiscali;
- fornire documentazione ed informazioni false nelle procedure di transazione fiscale.

A tal fine, devono essere messi in atto tutti i necessari controlli per la verifica preventiva delle informazioni disponibili sulle controparti commerciali prima di instaurare qualsiasi tipo di rapporto, con particolare attenzione alla verifica sulle società fornitrici e sulla sua effettiva operatività, nonché sulla coerenza dell'attività del fornitore con le prestazioni fatturate.

E' necessario verificare che il valore/prezzo dei beni o servizi acquistati sia in linea con quello di mercato e selezionare i fornitori in base a criteri oggettivi e di tracciare l'intero processo decisionale di ogni attività afferente il ciclo passivo e provvedere all'ordinata archiviazione della relativa documentazione, previa sua scrupolosa verifica.

In particolare, con riferimento ai pagamenti eseguiti o ricevuti a titolo di corrispettivo, sarà necessario che gli stessi siano conformi:

- (i) alle vendite/servizi effettivamente resi/ricevuti nonché
- (ii) alle pattuizioni contenute nel relativo contratto;

Inoltre, che tutti i pagamenti siano effettuati dietro emissione di fattura o documento equipollente, ove richiesto dalla legge e siano regolarmente contabilizzati conformemente alle disposizioni di legge applicabili.

Sarà altresì indispensabile custodire in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando adeguati mezzi fisici ed informatici che ne impediscano la distruzione o l'occultamento. Inoltre, vanno disposte verifiche periodiche sulle scritture contabili e garantita una segregazione di funzioni tra le attività di rilevazione/registrazione contabile delle operazioni aziendali da quelle di predisposizione delle dichiarazioni fiscali e conseguente calcolo e pagamento delle imposte.

All'uopo, è richiesto che sia applicato il corretto trattamento fiscale delle componenti di reddito, detrazioni e deduzioni secondo quanto previsto dalla normativa fiscale ed il rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette e indirette. Sarà opportuno curare la diffusione delle principali novità normative in materia fiscale al personale coinvolto nella gestione della fiscalità.

13.4 Procedure specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi.

13.4.1 Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze

Si rimanda alle Parti Speciali "REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE O DELL'UNIONE EUROPEA, REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA, REATI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI" e "REATI SOCIETARI" ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

13.4.2 Gestione dei rapporti con il Collegio Sindacale e la Società di Revisione

Si rimanda alla Parte Speciale "REATI SOCIETARI" ove sono già individuate le attività a rischio di commissione dei reati in oggetto e qualificati controlli e principi di comportamento aventi efficacia a presidio dei medesimi.

13.4.3 Gestione aspetti fiscali

La SGR, per lo svolgimento delle attività prodromiche all'esecuzione degli adempimenti fiscali opera con il supporto dell'outsourcer amministrativo, il quale fornisce di dati contabili necessari per procedere pagamento delle imposte e alla trasmissione delle dichiarazioni fiscali, così come prescritto dalla normativa tempo per tempo vigente.

Per l'adempimento degli obblighi fiscali previsti dalla normativa vigente in materia di IVA, ivi incluse le relative dichiarazioni annuali e periodiche, in materia di d'imposta ai fini IRES e IRAP e alla redazione delle corrispondenti dichiarazioni da presentare all'Amministrazione Finanziaria, nonché al versamento

degli acconti e dell'eventuale imposta dovuta a saldo, la SGR si avvale della collaborazione di un consulente fiscale esterno.

Il consulente fiscale inoltre:

- avvalendosi del supporto del Settore Amministrazione e Finanza, determina lo stanziamento per imposte dirette e indirette, ivi incluse quelle differite, da imputare nel bilancio della SGR;-
- monitora le variazioni della normativa fiscale eventualmente intervenute e determina le linee guida da adottare nel calcolo delle imposte, valutando le diverse opzioni nell'ambito del regime fiscale vigente, al fine di ottimizzare la gestione fiscale (tax planning);
- fornisce assistenza e consulenza su specifiche tematiche fiscali;
- gestisce i rapporti con l'Amministrazione Finanziaria in relazione alle richieste, verifiche, accertamenti di natura fiscale, nonché, gli adempimenti relativi agli eventuali contenziosi tributari.

Tutta la documentazione inerente ai pagamenti effettuati e ai relativi controlli è archiviata a cura dell'Ufficio Amministrazione in formato elettronico nella rete aziendale e/o cartaceo. Tale documentazione è a disposizione delle funzioni di controllo e dei revisori legali dei conti.

La SGR si è dotata di una specifica procedura aziendale in cui sono delineati i flussi operativi tra il Settore Amministrazione e il consulente fiscale nell'ambito dell'attività di gestione degli adempimenti fiscali.

La revisione dei bilanci della SGR è affidata ad una Società di Revisione in conformità alle disposizioni normative vigenti.

13.5 Controlli dell'Organismo di Vigilanza

Per la descrizione dei controlli suggeriti per specifici processi, si rimanda a quanto riportato nella Parte Speciale *"REATI SOCIETARI"*.