Quaestio Capital Management

Società di Gestione del Risparmio S.p.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

Revisione del Consiglio di Amministrazione di Quaestio Capital Management Società di Gestione del Risparmio S.p.A. in data 28.05.2025.

INDICE

1. PREMESSA

Il presente documento, corredato di tutti i suoi allegati, costituisce il Modello di Organizzazione, Gestione e Controllo (di seguito anche il "Modello") adottato da Quaestio Capital Management Società di Gestione del Risparmio S.p.A. (di seguito anche "Quaestio" o la "SGR" o la "Società") e rivisto con delibera del Consiglio di Amministrazione (di seguito anche "C.d.A.") del 21.4.2020, ai sensi del Decreto Legislativo 8 giugno 2001 n. 231 (di seguito denominato "Decreto" o "D.lgs. 231/2001").

Il Modello è così articolato:

- il contesto normativo di riferimento;
- la **Parte Generale**, che contiene:
  - il Modello di Governo della SGR e gli strumenti aziendali esistenti a supporto del Modello;
  - le finalità perseguite con l'adozione del Modello;
  - la metodologia adottata per l'analisi delle attività sensibili ai reati di cui al D.lgs. 231/2001 e dei relativi presidi;
  - l'individuazione e la nomina dell'Organismo di Vigilanza di Quaestio (di seguito anche "OdV" o "Organismo") con indicazione dei poteri, dei compiti e dei flussi informativi che lo riguardano;
  - il sistema disciplinare e il relativo apparato sanzionatorio;
  - il piano di informazione e formazione da adottare al fine di garantire la conoscenza delle misure e delle disposizioni del Modello;
  - i criteri di aggiornamento e adeguamento del Modello;
- la **Parte Speciale**, contenente i protocolli di decisione.

Costituiscono, inoltre, parte integrante del Modello i seguenti Allegati:

- Codice Etico e di Comportamento;
- Allegato "Elenco reati presupposto del D.lgs. 231/2001".

2. CONTESTO NORMATIVO

2.1. Natura e caratteristiche della responsabilità amministrativa prevista dal D.lgs. 231/2001

Il D.lgs. n. 231/2001, emanato l'8 giugno 2001, in attuazione della legge delega 29 settembre 2000, n. 300, disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (c.d. Enti[1]).

Tale legge delega ratifica, tra l'altro, la Convenzione sulla tutela finanziaria delle Comunità europee del 26 luglio 1995, la Convenzione U.E. del 26 maggio 1997 relativa alla lotta contro la corruzione e la Convenzione OCSE del 17 settembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali e ottempera agli obblighi previsti da siffatti strumenti internazionali e, in specie, comunitari i quali dispongono appunto la previsione di paradigmi di responsabilità delle persone giuridiche e di un corrispondente sistema sanzionatorio, che colpisca la criminalità d'impresa.

L'istituzione della responsabilità amministrativa delle società nasce dalla considerazione empirica che frequentemente le condotte illecite, commesse all'interno dell'impresa, lungi dal conseguire a un'iniziativa privata del singolo, rientrano piuttosto nell'ambito di una diffusa politica aziendale e conseguono a decisioni di vertice dell'Ente medesimo.

Si tratta di una responsabilità "amministrativa" *sui generis*, poiché, pur comportando sanzioni amministrative (si veda il successivo capitolo 2.4), consegue da reato e presenta le garanzie proprie del procedimento penale.

La sanzione amministrativa per gli Enti può essere applicata esclusivamente dal giudice penale e solo se sussistono tutti i requisiti oggettivi e soggettivi fissati dal legislatore: la commissione di determinati Reati elencati nel Decreto, nell'interesse[2] o a vantaggio[3] dell'Ente, da parte di:

- 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 (cosiddetti "Soggetti Apicali");
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (cosiddetti "Soggetti Sottoposti").

[1] Nell'ambito della definizione di Ente rientrano sia gli Enti dotati di personalità giuridica (S.p.A., S.r.l., società consortili, cooperative, associazioni riconosciute, fondazioni, altri enti privati e pubblici economici) sia gli Enti privi di personalità giuridica (Snc e Sas, consorzi, associazioni non riconosciute), mentre non vi rientrano lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici nonché gli enti che svolgono funzioni di rilievo costituzionale (art. 1, comma 3 del D.lgs. 231/2001).

[2] Favorire l'Ente, senza che sia in alcun modo necessario il conseguimento effettivo e concreto dell'obiettivo. Si tratta dunque di un criterio che si sostanzia nella finalità – anche non esclusiva – con la quale il Reato o l'Illecito è stato realizzato.

[3] Beneficio che l'Ente ha obiettivamente tratto dalla commissione del Reato o dell'Illecito, a prescindere dall'intenzione di chi l'ha commesso.

La responsabilità dell'Ente si aggiunge a quella della persona fisica che ha commesso materialmente l'illecito e sussiste in maniera autonoma rispetto a quest'ultima, anche quando l'autore materiale del reato non è stato identificato o non è imputabile ovvero nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

L'Ente, però, non è responsabile se il fatto illecito è stato commesso da uno dei soggetti indicati dal Decreto "nell'interesse esclusivo proprio o di terzi"[4].

Ai fini dell'affermazione della responsabilità dell'Ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'Ente, il legislatore impone l'accertamento della colpevolezza dell'Ente. Tale condizione si identifica con una colpa da organizzazione, intesa come violazione di adeguate regole di diligenza autoimposte dall'Ente medesimo e volte a prevenire lo specifico rischio da reato.

Specifiche disposizioni sono state dettate dal legislatore per i casi di trasformazione, fusione, scissione e cessione d'azienda per i quali si rimanda, per maggiori dettagli, a quanto specificamente previsto dagli artt. 28-33 del D.lgs. 231/2001.

2.2. Illeciti e reati che determinano la responsabilità amministrativa degli Enti

Originariamente prevista per i reati contro la Pubblica Amministrazione (di seguito anche "P.A.") o contro il patrimonio della P.A., la responsabilità dell'ente è stata estesa – per effetto di provvedimenti normativi successivi al D.lgs. 231/2001 – a numerosi altri reati e illeciti amministrativi. Relativamente proprio a questi ultimi, si precisa sin d'ora che, ogni qualvolta all'interno del presente documento si fa riferimento ai "reati presupposto" o "reati", tale riferimento è da intendersi comprensivo anche degli illeciti introdotti dal legislatore, quali ad esempio quelli previsti dalla normativa di *market abuse* (artt. 187 *bis* e 187 *ter*, per come richiamati dal Titolo I-bis del D.lgs. 58/98[5]).

Segnatamente, la responsabilità amministrativa degli enti può conseguire dai reati/illeciti elencati dal D.lgs. 231/2001, come di seguito riportati:

1) Reati contro la P.A. (artt. 24 e 25);
2) Reati informatici e trattamento illecito di dati (art. 24-bis);
3) Delitti di criminalità organizzata (art. 24-ter);

[4] La responsabilità dell'Ente si configura anche in relazione a Reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'Ente abbia nel territorio dello Stato italiano la sede principale.

[5] In diritto penale si definisce "reato" un fatto umano, commissivo o omissivo, al quale l'ordinamento giuridico ricollega una sanzione penale (vale a dire multa o ammenda, reclusione, arresto o ergastolo) in ragione del fatto che tale comportamento sia stato definito come antigiuridico perché costituisce un'offesa a un bene giuridico o un insieme di beni giuridici (che possono essere beni di natura patrimoniale o anche non patrimoniali) tutelati dall'ordinamento da una apposita norma incriminatrice. Rientra, quindi, nella più ampia categoria dell'illecito.

4) Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis);
5) Delitti contro l'industria e il commercio (art. 25-bis.1);
6) Reati societari (art. 25-ter);
7) Reati con finalità di terrorismo o di eversione dall'ordine democratico (art. 25-quater);
8) Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1);
9) Reati contro la personalità individuale (art. 25-quinquies);
10) Abusi di mercato (art. 25-sexies);
11) Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies);
12) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies);
13) Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1);
14) Delitti in materia di violazione del diritto d'autore (art. 25-novies);
15) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies);
16) Reati ambientali (art. 25-undecies);
17) Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies);
18) Reati di razzismo e xenofobia (art. 25-terdecies);
19) Reati transnazionali (art. 10 L. 16 marzo 2006, n. 146);
20) Frode in competizioni sportive, esercizio abusivo di giuoco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies);
21) Reati tributari (art. 25-quinquiesdecies);
22) Contrabbando (art. 25-sexiesdecies);
23) Delitti contro il patrimonio culturale (art. 25 septiesdecies);
24) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies).

Per maggiori dettagli si rimanda a quanto meglio specificato nell'Allegato del presente Modello "Elenco reati presupposto del D.lgs. n. 231/2001".

2.3. Adozione del Modello come possibile esimente della responsabilità amministrativa

Il Decreto prevede una forma specifica di esonero dalla responsabilità amministrativa dipendente dai Reati (c.d. condizione esimente), a seconda che il reato sia commesso dai Soggetti Apicali o dai Soggetti Sottoposti.

2.3.1. Reati e illeciti commessi dai Soggetti Apicali

Per i Reati commessi da Soggetti Apicali, l'Ente, per essere esente da colpa, dovrà dimostrare che (art. 6, comma 1 del D.lgs. n. 231/2001):

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire Reati della specie di quelli verificatisi;
- il compito di verificare il funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento, sia stato affidato ad un organo dell'Ente, dotato di autonomi poteri di iniziativa e controllo;
- le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il Modello;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'organo di cui al secondo punto.

Le condizioni sopra elencate devono concorrere tutte e congiuntamente affinché la responsabilità dell'Ente possa essere esclusa.

2.3.2. Reati e illeciti commessi dai Soggetti Sottoposti

Per i Reati commessi da Soggetti Sottoposti alla direzione o alla vigilanza di uno dei soggetti apicali, l'Ente è responsabile se la "commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza" dei soggetti apicali, inosservanza che è in ogni caso esclusa "se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire Reati della specie di quello verificatosi".

La responsabilità dell'Ente è pertanto ricondotta alla c.d. "colpa da organizzazione", ossia alla mancata adozione o al mancato rispetto di standard doverosi attinenti all'organizzazione e all'attività dell'Ente medesimo.

2.3.3. Efficace attuazione del Modello

L'art. 6, co. 1 del D.lgs. 231/2001 prevede la cosiddetta "condizione esimente", ovvero le condizioni che l'ente deve dimostrare per non essere imputabile della responsabilità ai sensi del D.lgs. 231/2001. In particolare l'ente non risponde della responsabilità ex D.lgs. 231/2001 se dimostra che l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi". Di conseguenza, la mera adozione del Modello non è sufficiente a garantire l'esonero dalla responsabilità per l'Ente, ma il Modello deve essere implementato nel rispetto delle seguenti condizioni previste dall'art. 6, co. 2 del Decreto:

- individuazione delle attività nel cui ambito esiste la possibilità che vengano commessi Reati previsti dal D.lgs. n. 231/2001;
- previsione di specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai Reati da prevenire;
- individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione di Reati;
- previsione degli obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introduzione di un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Il Modello deve altresì prevedere:

- uno o più canali che consentano ai Soggetti Apicali ed ai Soggetti Sottoposti di inoltrare segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto, e tali da garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Deve inoltre rispondere al requisito dell'efficace attuazione, il quale, come previsto dall'art. 7, co. 4 del D.lgs. 231/2001, richiede fra l'altro la verifica periodica nonché l'eventuale modifica del Modello, ogniqualvolta l'Ente modifichi la propria struttura organizzativa o l'oggetto delle attività sociali o si rilevino significative violazioni delle prescrizioni.

2.4. Sanzioni irrogabili all'Ente

A carico dell'Ente che ha tratto vantaggio dalla commissione del reato, o nel cui interesse sono stati compiuti i Reati, sono irrogabili (art. 9 del D.lgs. n. 231/2001) le seguenti misure sanzionatorie:

- sanzione pecuniaria: si applica ogniqualvolta è riconosciuta la responsabilità dell'Ente ed è determinata dal giudice penale attraverso un sistema basato su "quote". Per i Reati previsti dall'art. 25-sexies del D.lgs. n. 231/2001 e gli Illeciti Amministrativi di cui all'art. 187-quinquies del TUF, se il prodotto o il profitto conseguito dall'Ente è di rilevante entità "la sanzione pecuniaria è aumentata fino a dieci volte tale prodotto o profitto".

Il Decreto prevede altresì l'ipotesi di riduzione della sanzione pecuniaria, allorquando l'autore del Reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne abbia ricavato un vantaggio ovvero ne abbia ricavato un vantaggio minimo, oppure quando il danno cagionato risulti di particolare tenuità.

La sanzione pecuniaria, inoltre, è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado, l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del Reato, o si è comunque adoperato in tal senso. La sanzione pecuniaria è poi ridotta anche nel caso in cui l'Ente abbia adottato e reso operativo, prima della dichiarazione di apertura del dibattimento di primo grado, un modello idoneo alla prevenzione di Reati della specie di quello verificatosi.

Del pagamento della sanzione pecuniaria inflitta risponde soltanto l'Ente, con il suo patrimonio; si esclude, pertanto, una responsabilità patrimoniale diretta dei soci o degli associati, indipendentemente dalla natura giuridica dell'Ente;

- sanzione interdittiva: si applica per alcune tipologie di Reati e per le ipotesi di maggior gravità. Si traduce:
  - nell'interdizione dall'esercizio dell'attività aziendale;
  - nella sospensione e nella revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell'illecito;
  - nel divieto di contrattare con la Pubblica Amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio);
  - nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli concessi;
  - nel divieto di pubblicizzare beni o servizi.

  In ogni caso, le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) qualora l'Ente – prima della dichiarazione di apertura del dibattimento di primo grado:
  - abbia risarcito integralmente il danno, o lo abbia riparato;
  - abbia eliminato le conseguenze dannose o pericolose del Reato (o, almeno, si sia adoperato in tal senso);
  - abbia messo a disposizione dell'Autorità Giudiziaria, per la confisca, il profitto del Reato;
  - abbia eliminato le carenze organizzative che hanno determinato il Reato, adottando e attuando modelli organizzativi idonei a prevenire la commissione di nuovi Reati.

Qualora ricorrano tutti questi comportamenti – considerati di ravvedimento operoso – anziché la sanzione interdittiva si applicherà quella pecuniaria:

- confisca: consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato o nell'acquisizione di somme di danaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato; non investe, tuttavia, quella parte

del prezzo o del profitto del reato che può restituirsi al danneggiato. La confisca è sempre disposta con la sentenza di condanna;

- pubblicazione della sentenza: può essere disposta quando all'Ente viene applicata una sanzione interdittiva; viene effettuata a cura della cancelleria del Giudice, a spese dell'Ente, ai sensi dell'articolo 36 del codice penale, nonché mediante affissione nel comune ove l'Ente ha la sede principale[6].

[6] La Legge Finanziaria di Luglio 2011 ha modificato l'art. 36 del Codice Penale, richiamato dall'art. 18 del D. Lgs. 231/2001. A seguito di tale modifica, la sanzione relativa alla "pubblicazione della sentenza penale di condanna" è stata ridotta in termini di severità, prevedendo che la pubblicazione avverrà esclusivamente nel sito del Ministero della Giustizia e non anche nei quotidiani nazionali.

PARTE GENERALE

3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI QUAESTIO

3.1. Quaestio Capital Management Società di Gestione del Risparmio S.p.A.

Quaestio è una società di gestione del risparmio indipendente, specializzata sin dal 2009 in clientela istituzionale, che opera con un'ottica globale, identificando e gestendo le migliori idee di investimento sui principali mercati del mondo.

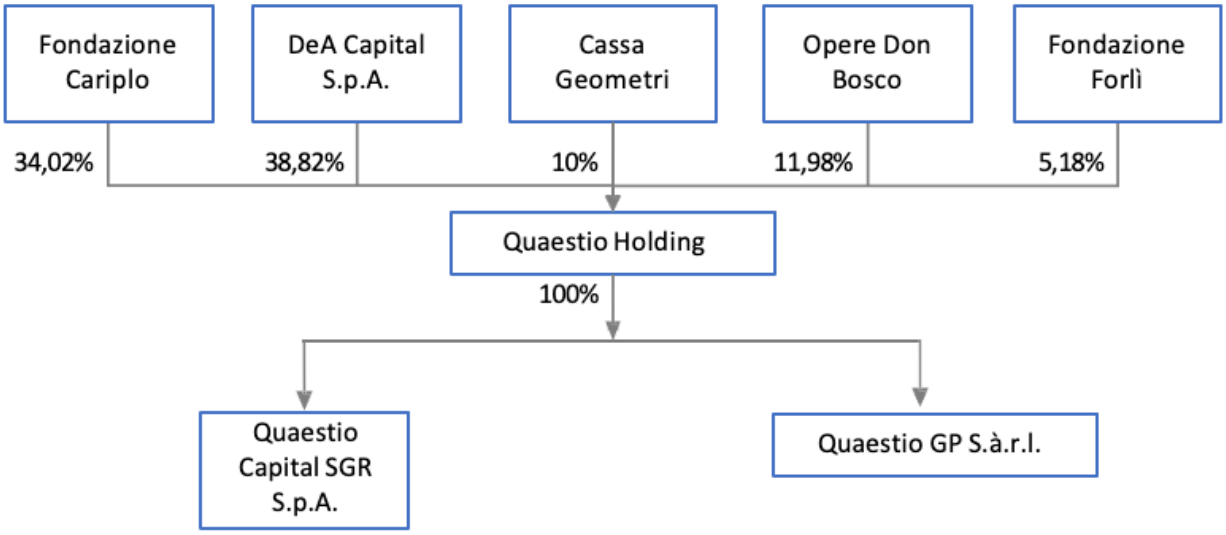
La SGR istituisce e gestisce sia fondi UCITS che FIA di diritto italiano e lussemburghese e fornisce, inoltre, servizi di gestione patrimoniale individuale.

Quaestio è detenuta interamente da Quaestio Holding S.A., società lussemburghese che detiene altresì il 100% di Quaestio GP S.à.r.l., società di diritto lussemburghese, che svolge il ruolo di general partner di due Sicav di diritto lussemburghese.

La compagine sociale di Quaestio Holding S.A. è così ripartita: (i) 38,82% DeA Capital S.p.A, (ii) 34,02% Fondazione Cariplo, (iii) 11,98% Direzione Generale Opere Don Bosco, (iv) 10% Cassa Italiana di Previdenza ed Assistenza dei Geometri Liberi Professionisti e (v) 5,18% Fondazione Cassa dei Risparmi di Forlì.

Nessuno dei soci sopra indicati esercita il controllo della Quaestio Holding S.A., essendo richiesta dallo statuto la maggioranza del capitale per le delibere dell'assemblea ordinaria e i due terzi degli azionisti (presenti o rappresentati) per quelle dell'assemblea straordinaria.

Si riporta di seguito l'attuale rappresentazione grafica della struttura di controllo:



3.2. Funzione e scopo del Modello

Benché la legge non ne preveda l'obbligo, Quaestio ha ritenuto opportuno adottare uno specifico Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001, conforme alle indicazioni del Decreto, nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione di tutti coloro che operano per conto della SGR, affinché tengano comportamenti corretti e lineari, anche un più efficace mezzo di prevenzione contro il rischio di commissione dei Reati e degli Illeciti di cui al Decreto.

In particolare, attraverso l'adozione del presente Modello, la SGR intende perseguire le seguenti finalità:

- adeguarsi alla normativa sulla responsabilità amministrativa degli Enti, nonché verificare e valorizzare i presidi già in essere, atti a prevenire la realizzazione di condotte illecite rilevanti ai sensi del D.lgs. 231/2001;
- informare tutti coloro che operano per conto della SGR del contenuto del Decreto, della sua rilevanza e delle sanzioni penali e amministrative che possono essere comminate alla SGR e nei loro confronti, in caso di violazione degli obblighi impartiti in materia, nonché delle conseguenze disciplinari e/o contrattuali che possono derivarne nei loro confronti;
- rendere noto che Quaestio non tollera condotte che, anche se possono apparentemente favorire l'interesse della SGR, sono contrarie, oltre che alle disposizioni di legge, alla normativa di settore e aziendale, anche ai principi etici ai quali la SGR intende attenersi nell'esercizio dell'attività aziendale;
- assumere le iniziative necessarie per prevenire o contrastare comportamenti illeciti e contrari al proprio Modello.

Il Modello di Quaestio:

- è costituito dall'insieme delle regole interne di cui la SGR si è dotata, in relazione ai rischi connessi all'attività specifica svolta;
- individua le attività nel cui ambito possono essere commessi i Reati e gli Illeciti e definisce i principi comportamentali necessari per evitare che siano commessi;
- si poggia sui principi fondamentali della:
  - trasparenza dei comportamenti riferibili alle aree sensibili, come di seguito individuate, sia all'interno di Quaestio che nei rapporti con le controparti esterne;
  - tracciabilità delle operazioni relative alle aree sensibili, finalizzata a garantire la verificabilità delle congruenze e coerenza delle stesse, anche attraverso un adeguato supporto documentale;

- correttezza da parte di tutti i soggetti facenti capo a Quaestio, garantita dal rispetto delle disposizioni di legge, di regolamenti, della normativa e delle procedure organizzative interne.

3.3. Destinatari

I principi e le disposizioni del Modello devono essere rispettati da tutti i soggetti interni alla SGR, nonché da tutti i soggetti esterni che, in forza di rapporti contrattuali, prestino la loro collaborazione a Quaestio per la realizzazione delle sue attività, intendendosi per:

- soggetti interni:
  - componenti degli Organi sociali della SGR;
  - tutto il Personale della SGR intendendosi per tale:
    - i dipendenti, compreso il top management;
    - i collaboratori legati da contratto dipendente a termine;
- soggetti esterni, nei limiti del rapporto in essere con la SGR, quali a titolo esemplificativo e non esaustivo:
  - i lavoratori autonomi o parasubordinati;
  - i fornitori di beni e servizi, inclusi professionisti e consulenti;
  - gli agenti;
  - i partner commerciali.

La SGR richiede ai soggetti esterni il rispetto del Modello, nonché del Codice Etico e di Comportamento, ove possibile anche mediante l'apposizione di una clausola contrattuale che impegni il contraente ad attenersi ai principi di cui al D.Lgs 231/01.

Ai fini del Modello Quaestio considera Soggetti Apicali:

- i componenti degli Organi sociali della SGR;
- i responsabili di Area/Funzione/Unità della SGR, come definiti dall'organigramma *pro tempore* vigente.

Gli altri soggetti interni ed esterni sono considerati Soggetti Sottoposti.

L'insieme dei soggetti interni e dei soggetti esterni costituisce i "Destinatari" del Modello.

3.4. Modello di governance di Quaestio e strumenti aziendali esistenti a supporto del Modello

Il presente Modello si integra all'interno della normativa, delle procedure e dei sistemi di controllo già esistenti ed operanti in Quaestio.

Il contesto organizzativo della SGR è costituito dall'insieme di regole, strutture e procedure che ne garantiscono il corretto funzionamento; si tratta dunque di un sistema articolato che rappresenta già di per sé uno strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

In particolare, quali specifici strumenti diretti a programmare la formazione e l'attuazione delle decisioni aziendali e a effettuare i controlli, la SGR ha individuato:

- le regole di corporate governance;
- il Sistema dei Controlli Interni;
- il sistema dei poteri e delle deleghe;
- il Codice Etico e di Comportamento.

Inoltre, la SGR ha formalizzato in specifici protocolli di decisione:

- il risultato della ricognizione delle "attività sensibili" nell'ambito delle quali può verificarsi il rischio di commissione dei reati presupposto;
- i principi di comportamento e le regole di controllo volti a prevenire i reati.

3.4.1. Modello di governance e struttura organizzativa di Quaestio

Quaestio adotta, fin dalla sua costituzione, il sistema di amministrazione cosiddetto tradizionale.

Caratteristica essenziale di tale sistema è la separazione tra i compiti di gestione della società, di controllo sull'amministrazione e di revisione legale dei conti.

Al vertice della struttura della SGR vi è il Consiglio di Amministrazione, di nomina assembleare, a cui spetta in via esclusiva la supervisione strategica e la gestione dell'impresa. Al Collegio Sindacale, anch'esso di nomina assembleare, spetta il controllo sull'amministrazione mentre la revisione legale è affidata, dall'Assemblea su proposta motivata del Collegio Sindacale, a una società di revisione legale.

A sua volta, il Consiglio di Amministrazione ha conferito poteri di rappresentanza e parte delle proprie attribuzioni ad un Amministratore Delegato, con estesi poteri di gestione, e ad alcuni procuratori, con poteri di rappresentanza specifici. Infine, ampi poteri vicari, da esercitarsi in via di urgenza, sono permessi dallo statuto sociale al Presidente e all'Amministratore Delegato.

La Società ha istituito al suo interno i comitati di seguito elencati:

- tre comitati endo-consiliari in linea con il Regolamento della Banca d'Italia del 5.12.2019 e precisamente un Comitato Remunerazioni, o RemCo, un Comitato Controlli interni e Rischi e un Comitato Nomine ed ESG;
- due comitati di investimento, ciascuno competente per ogni ambito di investimento della SGR nonché per le proposte di governo dei prodotti nei confronti del Consiglio di Amministrazione;
- un comitato dedicato alla gestione e l'ottimizzazione delle tematiche riguardanti le attività della SGR sugli Investimenti Sostenibili.

Da un punto di vista organizzativo, la struttura della SGR è di tipo gerarchico-piramidale. In particolare:

- sono presenti più Unità organizzative le quali riportano gerarchicamente alla competente Area;
- le Aree della SGR riportano all'Amministratore Delegato (l'Area controlli funzionalmente anche al Comitato Controlli Interni e Rischi), il quale svolge anche funzioni di raccordo tra il Consiglio di Amministrazione e i comitati di investimento.

La struttura organizzativa della SGR trova rappresentazione nell'organigramma *pro tempore* vigente.

3.4.2. Sistema dei Controlli Interni

La SGR ha istituito un proprio Sistema dei Controlli Interni, costituito dall'insieme di regole, funzioni, strutture, risorse, processi e procedure volti alla verifica dell'attuazione delle strategie e politiche aziendali, all'efficienza ed efficacia dei processi aziendali, al mantenimento dell'affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche e alla identificazione, misurazione o valutazione, prevenzione o attenuazione e comunicazione dei rischi rilevanti in riferimento alla SGR e ai fondi e portafogli dalla stessa gestiti.

l Sistema dei Controlli Interni della SGR è articolato nei seguenti livelli di controllo:

- controlli di primo livello (controlli di linea), i quali si sostanziano in verifiche poste in essere direttamente dalle aree della SGR e diretti ad assicurare il corretto svolgimento delle operazioni;
- controlli di secondo livello, intendendosi per tali i controlli inerenti alla gestione dei rischi a cui può essere soggetta la SGR (risk management), i controlli di conformità alle norme (compliance), volti a prevenire il rischio di non conformità alle norme applicabili nell'ambito della prestazione dei servizi propri della SGR, nonché i controlli implementati ai sensi della normativa vigente in materia di prevenzione e contrasto al riciclaggio e al finanziamento del terrorismo (antiriciclaggio);
- controlli di terzo livello, ossia i controlli di revisione interna (internal auditing), finalizzati alla valutazione della completezza, della funzionalità e dell'adeguatezza dei sistemi e delle procedure, anche di controllo, della SGR.

Per quanto concerne i controlli di primo livello, questi caratterizzano tutti i processi aziendali e sono di competenza delle aree operative della SGR.

Con riferimento, invece, ai controlli di secondo livello, la SGR ha istituito un'Area Controlli, con a capo un Chief Risk Officer (o "CRO") e composta dall'unità di financial e ITC risk management (o "FRM"), dall'unità di compliance e dall'unità di AML/SOS; come più sopra indicato l'Area riporta gerarchicamente all'Amministratore delegato e funzionalmente al Comitato Controlli Interni e Rischi. Il CRO collabora, insieme alle altre Funzioni, al Datore di lavoro e al Committente ai sensi del D.lgs. n. 81/2008, per quanto di loro competenza, all'aggiornamento del Modello in coerenza con l'evoluzione della normativa di riferimento e con le modifiche della struttura organizzativa aziendale.

In particolare, la FRM presidia il processo di gestione e monitoraggio dei rischi di credito, operativi e reputazionali, sviluppando e convalidando principi, metodologie e modelli di misurazione e controllo degli stessi. L'unità ha accesso a tutte le informazioni pertinenti per l'assolvimento dei compiti e delle attività di seguito riportate:

- individuazione, misurazione, gestione e monitoraggio dei rischi a cui i portafogli sono o potrebbero essere esposti;
- monitoraggio dei limiti di rischio previsti con riferimento a ciascun portafoglio e verifica della conformità di tali limiti con il profilo di rischio dei portafogli gestiti;
- aggiornamento periodico al Consiglio di Amministrazione circa i rischi dei portafogli e d'impresa e l'adeguatezza e l'efficacia del processo di gestione del rischio.

L'unità di Compliance ha il compito specifico di verificare che le procedure interne siano coerenti con l'obiettivo di prevenire la violazione di norme, regolamenti e disposizioni interne applicabili alla SGR. Alla funzione sono attribuiti i seguenti compiti:

- controllare e valutare periodicamente l'adeguatezza e l'efficacia delle misure, delle politiche e delle procedure messe in atto dalla SGR al fine di:
  - individuare il rischio di mancata osservanza degli obblighi posti dalle vigenti disposizioni normative in materia di gestione collettiva e di servizi e attività di investimento, nonché i rischi che ne derivano;
  - minimizzare tale rischio e consentire alle autorità competenti di esercitare efficacemente i poteri ad essi conferiti dalle vigenti disposizioni normative;
- individuazione dei rischi d'impresa a cui la SGR è esposta per il tramite di un apposito Compliance & Risk Assessment;
- adottare misure adeguate per rimediare a eventuali carenze nell'adempimento degli obblighi da parte della stessa;
- fornire consulenza ai soggetti rilevanti nella prestazione dei servizi e nell'esercizio delle attività e assisterli ai fini dell'adempimento degli obblighi posti dalle vigenti disposizioni normative.

L'unità di compliance/AML fornisce una costante assistenza per l'adempimento degli obblighi in materia di antiriciclaggio e sottopone almeno annualmente al Consiglio di Amministrazione relazioni sull'attività e sulle verifiche svolte.

Infine, per quanto concerne i controlli di terzo livello, gli stessi sono svolti dalla funzione Internal Audit, integralmente esternalizzata, la quale riporta direttamente al Consiglio di Amministrazione della SGR. Tale funzione ha il compito di supportare il management aziendale nell'attività di mitigazione dei rischi e nell'adempimento delle proprie responsabilità, attraverso la revisione delle attività e delle procedure relative a tutte le aree aziendali, con l'obiettivo di:

- salvaguardare il patrimonio aziendale;
- verificare l'adeguatezza e l'efficacia del sistema dei controlli interni;
- verificare l'adeguatezza e l'efficacia del sistema di gestione/ controllo dei rischi;
- verificare il rispetto delle procedure organizzative aziendali adottate;
- favorire l'utilizzo adeguato e ottimale delle risorse.

In materia di prevenzione e contrasto dell'utilizzo del sistema finanziario per finalità di riciclaggio e di finanziamento del terrorismo, la funzione vigila sull'osservanza delle disposizioni normative e delle procedure interne.

Inoltre, la funzione svolge un'attività di supporto di tipo consultivo ai settori dell'organizzazione aziendale con riferimento alle problematiche concernenti la prestazione dei servizi, i conflitti di interessi e i conseguenti comportamenti da tenere.

3.4.3. Sistema dei poteri e delle deleghe

Quaestio ha strutturato un sistema coerente di deleghe e di sub-deleghe all'interno del quale sono individuati, in modo analitico e caratterizzato da chiarezza e precisione, i poteri che il Consiglio di Amministrazione delega all'Amministratore Delegato e ai responsabili e/o altri soggetti delle aree della SGR, unitamente ai limiti quantitativi[7] e qualitativi[8], nonché alle relative modalità di esercizio da parte dei soggetti delegati. Ampi poteri vicari di emergenza sono conferiti dallo statuto al Presidente del Consiglio e all'Amministratore Delegato.

Al fine di garantire coerenza all'intero sistema:

- i poteri sono stati assegnati in maniera graduata;
- l'assunzione di decisioni eccedenti i limiti quantitativi/qualitativi delle deleghe attribuite necessita del preventivo parere del livello gerarchico superiore.

[7] Per limiti quantitativi / di valore si intendono i limiti di importo delle singole operazioni che ciascun soggetto delegato può autorizzare.

[8] I limiti qualitativi sono volti a limitare l'operatività del singolo soggetto delegato a specifiche e definite attività.

La Società ha altresì definito un processo di gestione e autorizzazione delle spese garantendo il rispetto dei principi di trasparenza, verificabilità, inerenza all'attività aziendale e la coerenza fra i poteri autorizzativi di spesa e le responsabilità organizzative e gestionali.

3.4.4. Codice Etico e di Comportamento

La SGR, riconoscendo e promuovendo i più elevati standard di comportamento, ha declinato, all'interno del proprio Codice Etico e di Comportamento, l'insieme dei valori e dei principi, nonché le linee di comportamento a cui devono attenersi i vertici aziendali di Quaestio, tutte le persone legate alla stessa da rapporti di lavoro nonché tutti coloro che operano per la Società, quale che sia il rapporto che li lega alla medesima.

Il Codice Etico e di Comportamento costituisce presupposto e parte integrante del presente Modello.

4. ADOZIONE, EFFICACE ATTUAZIONE, MODIFICAZIONE E AGGIORNAMENTO DEL MODELLO

4.1. Adozione del Modello

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

In fase di adozione del Modello, l'Amministratore Delegato definisce la struttura del Modello da sottoporre all'approvazione del Consiglio di Amministrazione con il supporto, per gli ambiti di rispettiva competenza, delle aree aziendali e dell'Organismo di Vigilanza.

4.2. Efficace attuazione, modificazione e aggiornamento del Modello

Il Consiglio di Amministrazione, modifica il Modello qualora siano state individuate significative violazioni delle prescrizioni in esso contenute che ne evidenziano l'inadeguatezza, anche solo parziale, a garantire l'efficace prevenzione dei Reati di cui al Decreto e aggiorna, in tutto o in parte, i contenuti del Modello qualora intervengano mutamenti nell'organizzazione, nell'attività o nel contesto normativo di riferimento.

Le modifiche o gli aggiornamenti meramente formali del presente documento e/o delle singole Parti Speciali sono rimessi all'autonomia dell'Amministratore Delegato, fermi restando tutti gli obblighi informativi.

L'efficace e concreta attuazione del Modello è garantita altresì dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle singole funzioni aziendali, nonché dagli organi aziendali e dai responsabili delle varie aree aziendali, i quali propongono alle competenti aree le modifiche delle procedure di loro competenza, quando tali modifiche appaiano necessarie per l'efficace attuazione del Modello.

È facoltà comunque dell'Organismo di Vigilanza proporre al Consiglio di Amministrazione (ovvero alle strutture societarie competenti) le variazioni ritenute necessarie ai protocolli e ai flussi informativi da / verso l'Organismo di Vigilanza.

Nella gestione del Modello sono inoltre coinvolte le funzioni di seguito indicate, a cui sono affidati, in tale ambito, specifici ruoli e responsabilità.

Si rileva che nel prosieguo del presente documento sarà utilizzato il termine "funzione" per indicare indistintamente le Funzioni/Aree/Unità previste dall'organigramma della SGR.

Funzione Internal Audit

La funzione Internal Audit, integralmente esternalizzata, collabora con l'Organismo di Vigilanza ai fini dell'espletamento delle sue attività di controllo, portando all'attenzione dello stesso eventuali criticità riscontrate nel corso delle proprie attività di verifica di terzo livello, con particolare riferimento a quelle potenzialmente connesse a profili di rischio di

commissione di reati rilevanti ai sensi del Decreto, nonché monitorando che le funzioni competenti portino a termine le azioni di mitigazione individuate a fronte di tali criticità.

Unità di Compliance/AML/SOS

Le unità di compliance/AML/SOS attraverso i propri responsabili supportano direttamente l'attività di controllo dell'Organismo di Vigilanza, monitorando nel tempo l'efficacia delle regole e dei principi di comportamento indicati nel Modello a prevenire i Reati di cui al Decreto e porta all'attenzione dello stesso Organismo eventuali criticità riscontrate nel corso delle proprie attività di verifica di secondo livello, con particolare riferimento a quelle potenzialmente connesse a profili di rischio di commissione di reati rilevanti ai sensi del Decreto, nonché monitora che le funzioni competenti portino a termine le azioni di mitigazione individuate a fronte di tali criticità.

L'unità di Compliance, inoltre:

- programma interventi di formazione e sensibilizzazione rivolti a tutti i dipendenti sull'importanza di un comportamento conforme alle regole aziendali nonché specifici corsi destinati al personale che opera nelle attività sensibili con lo scopo di chiarire in dettaglio le criticità, i segnali premonitori di anomalie o irregolarità, le azioni correttive da implementare per le operazioni anomale o a rischio;
- presidia, con il supporto delle funzioni Internal Audit e l'area Legal, il processo di rilevazione e gestione delle violazioni del Modello, nonché il conseguente processo sanzionatorio - di concerto con l'Amministratore Delegato - e, a sua volta, fornisce tutte le informazioni emerse in relazione ai fatti e/o ai comportamenti rilevanti ai fini del rispetto della normativa del Decreto all'Organismo di Vigilanza, il quale le analizza al fine di prevenire future violazioni, nonché di monitorare l'adeguatezza del Modello.

La funzione partecipa inoltre – sempre per gli ambiti di sua competenza e in raccordo con le altre funzioni aziendali competenti in materia di formazione – alla predisposizione di un adeguato piano formativo.

Financial e ITC risk management (FRM)

La FRM assicura puntuali flussi informativi all'Organismo di Vigilanza in merito a carenze nel sistema di gestione dei rischi, eventualmente rilevate nel corso delle proprie attività di verifica, che possano compromettere la corretta attuazione del Modello. In relazione a tali eventuali carenze, tiene altresì informato l'Organismo di Vigilanza circa lo stato di implementazione delle connesse azioni di mitigazione individuate.

Area Legal

Per il perseguimento delle finalità di cui al Decreto, l'area Legal collabora con le altre Funzioni aziendali, con il Datore di lavoro e il Committente ai sensi del D.lgs. n. 81/2008 alla corretta applicazione del Modello in coerenza con l'evoluzione della normativa di riferimento e con le modifiche della struttura organizzativa aziendale.

Area HR

L'area HR al fine di meglio presidiare la coerenza della struttura organizzativa e dei meccanismi di governance rispetto agli obiettivi perseguiti col Modello, ha la responsabilità di diffondere la normativa interna a tutta la Società.

Datore di lavoro e Committente ai sensi del D.lgs. n. 81/2008

Il Datore di Lavoro e il Committente ai sensi del D.lgs. n. 81/2008, limitatamente all'ambito di competenza per la gestione dei rischi in materia di salute e sicurezza nei luoghi di lavoro, individuano e valutano l'insorgenza di fattori di rischio dai quali possa derivare la commissione di Reati di cui al Decreto e promuovono eventuali modifiche organizzative volte a garantire un presidio dei rischi individuati. Per gli ambiti di propria competenza, essi possono partecipare alla definizione della struttura del Modello e all'aggiornamento dello stesso, nonché alla predisposizione del piano di formazione.

Nell'ambito della SGR, il ruolo e le funzioni del Datore di Lavoro e del Committente sono in capo all'intero Consiglio di Amministrazione.

Altre Funzioni della SGR

Alle varie Funzioni della SGR è assegnata la responsabilità dell'esecuzione, del buon funzionamento e dell'efficace applicazione nel tempo dei processi. La normativa interna individua le aree cui è assegnata la responsabilità della progettazione dei processi.

Per i specifici fini del Decreto, le varie Funzioni hanno la responsabilità di:

- rivedere, alla luce dei principi di controllo e di comportamento prescritti per la disciplina delle attività sensibili, le prassi e i processi di propria competenza, al fine di renderli adeguati a prevenire comportamenti illeciti;
- segnalare all'Organismo di Vigilanza eventuali situazioni di irregolarità o comportamenti anomali.

In particolare, le predette Funzioni per le attività aziendali sensibili devono prestare la massima e costante cura nel verificare l'esistenza e nel porre rimedio a eventuali carenze di normative o di procedure che potrebbero dar luogo a prevedibili rischi di commissione di illeciti presupposto nell'ambito delle attività di propria competenza.

4.3. Modalità operative seguite per la costruzione e l'aggiornamento del Modello

Si è provveduto a identificare i principi di comportamento e le regole di controllo volti a prevenire la commissione dei reati presupposto e a formalizzarli in specifici protocolli di decisione rispondenti all'operatività delle strutture organizzative e avendo riguardo alle specificità di ogni settore di attività.

Si richiamano anche le Linee Guida dell'Associazione Confindustria, indicative di *best practice* applicabili alla generalità dei Modelli ex D.lgs. 231/2001 a prescindere del settore di attività dell'ente e che sono state altresì considerate nell'ambito della metodologia di risk assessment & gap analysis adottata nell'aggiornamento del Modello della SGR.

Gli interventi di predisposizione e successivo aggiornamento del Modello si basano su una metodologia uniforme che prevede la realizzazione delle seguenti attività:

Fase I - Raccolta e analisi della documentazione

Al fine di una puntuale comprensione del sistema di governance e controllo in essere presso la SGR, si è proceduto ad analizzare l'insieme dei documenti in vigore presso la stessa che forniscono le indicazioni circa il sistema di regole e normative a governo dei processi aziendali. Particolare attenzione è stata attribuita all'analisi della seguente documentazione:

- organigramma e documenti descrittivi delle funzioni della struttura organizzativa (in particolare, Relazione sulla struttura organizzativa e sull'assetto contabile);
- sistema dei poteri e delle deleghe;
- Codice Etico e di Comportamento;
- policy e procedure operative;
- sistema sanzionatorio esistente.

Fase II - Identificazione delle attività "sensibili" e dei presidi in essere

Successivamente alla raccolta di tutto il materiale di cui alla Fase I, si è proceduto – tenuto conto della specifica operatività della SGR e nell'ambito della conduzione dell' Compliance & Risk Assessment – alla individuazione e rappresentazione in apposite schede di risk assessment & gap analysis delle attività "sensibili" o "a rischio" di realizzazione dei reati richiamati dal D.lgs. 231/2001, nonché degli illeciti amministrativi di cui al TUF per i quali trova applicazione il Decreto.

Una volta identificate le attività sensibili, sono stati rilevati – tramite analisi documentale e interviste ai responsabili delle Funzioni della SGR – i presidi di controllo in essere aventi efficacia in termini di prevenzione dei rischi-reato, verificando quindi l'adeguatezza degli stessi presidi e individuando eventuali ambiti di rafforzamento. Le relative risultanze sono state documentate nelle schede di risk assessment & gap analysis ed archiviate.

Fase III - Elaborazione dei protocolli

I protocolli, riportati nella Parte Speciale del Modello, contengono i principi di controllo e di comportamento definiti con l'obiettivo di stabilire le regole, a cui la SGR deve adeguarsi con riferimento all'espletamento delle attività definite sensibili.

La scelta di seguire tale approccio è stata effettuata considerando che tale modalità consente di valorizzare al meglio il patrimonio conoscitivo della SGR in termini di regole e normative interne che indirizzano e governano la formazione e l'attuazione delle decisioni della SGR in relazione agli illeciti da prevenire e, più in generale, la gestione dei rischi e

l'effettuazione dei controlli. Inoltre tale approccio permette di gestire con criteri univoci le regole operative aziendali, incluse quelle relative alle aree "sensibili" e, da ultimo, rende più agevole la costante implementazione e l'adeguamento tempestivo dei processi e dell'impianto normativo interni ai mutamenti della struttura organizzativa e dell'operatività aziendale, assicurando un elevato grado di "dinamicità" del Modello.

Il presidio dei rischi rivenienti dal D.lgs. 231/2001 è pertanto assicurato dal presente documento ("Modello di Organizzazione, Gestione e Controllo") e dall'impianto normativo esistente, che ne costituisce parte integrante e sostanziale.

5. ORGANISMO DI VIGILANZA

5.1. Composizione e nomina

L'Organismo di Vigilanza si identifica in un organismo collegiale *ad hoc*, composto da tre membri effettivi individuati come segue:

- un membro esterno in qualità di Presidente;
- il responsabile della funzione Internal Audit;
- un membro in possesso di adeguate conoscenze specialistiche.

In attuazione di quanto previsto dal Decreto e in coerenza con le norme statutarie, il Consiglio di Amministrazione della SGR nomina l'Organismo di Vigilanza e il suo Presidente.

La rinuncia da parte dei componenti dell'Organismo di Vigilanza può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione, per iscritto, unitamente alle motivazioni che l'hanno determinata.

La durata in carica dei membri dell'Organismo di Vigilanza coincide, ove non diversamente previsto, con quella del Consiglio di Amministrazione che l'ha nominato e i suoi membri possono essere rieletti. Il funzionamento dell'Organismo di Vigilanza può essere disciplinato da un eventuale Regolamento, approvato dal medesimo Organismo.

La nomina quale componente dell'Organismo di Vigilanza è condizionata, in particolare, alla presenza di requisiti soggettivi di eleggibilità, di seguito descritti.

5.2. Requisiti di eleggibilità, cause di decadenza e sospensione, temporaneo impedimento

Requisiti soggettivi di eleggibilità

I membri esterni:

- devono essere scelti tra esperti in materie giuridiche, economiche, finanziarie, tecnico-scientifiche o comunque tra soggetti in possesso di idonee competenze specialistiche adeguate alla funzione derivanti, ad esempio, dall'avere svolto per un congruo periodo di tempo attività professionali in materie attinenti il settore nel quale la Società opera e/o dall'avere un'adeguata conoscenza dell'organizzazione e dei principali processi aziendali;
- non devono avere vincoli di parentela con gli esponenti e con il top management appartenenti al vertice della Società, né devono essere legati alla stessa da rapporti di lavoro autonomo, ovvero da altri significativi rapporti di natura patrimoniale o professionale che ne compromettano l'indipendenza.

Costituiscono motivi di ineleggibilità e/o di decadenza dei componenti dell'OdV di Quaestio:

- trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile;
- avere titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una influenza su Quaestio o su Quaestio Holding S.A. e sulle altre società nelle quali Quaestio Holding S.A. detiene una partecipazione;
- essere stato sottoposto a misure di prevenzione ai sensi della legge 27 dicembre 1956, n. 1423 o della legge 31 maggio 1965, n. 575 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- aver riportato sentenza di condanna o patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
  - per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
  - per uno dei delitti previsti dal titolo XI del Libro V del codice civile (società e consorzi);
  - per un delitto non colposo, per un tempo non inferiore a un anno;
  - per un delitto contro la P.A., contro la fede pubblica, contro il patrimonio, contro l'economia pubblica ovvero per un delitto in materia tributaria;
  - per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento.
- aver riportato, in Italia o all'estero, sentenza di condanna o di patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex D.lgs. 231/2001;
- essere destinatario di un decreto che dispone il giudizio per tutti i reati/illeciti previsti dal D.lgs. 231/2001.

Autonomia e indipendenza

L'autonomia e l'indipendenza dell'OdV sono garantite dall'autonomia dell'iniziativa di controllo rispetto a ogni forma d'interferenza o di condizionamento da parte di qualunque esponente della persona giuridica e, in particolare, dell'organo dirigente. Al fine di assicurare tali requisiti, l'OdV riporta esclusivamente al Consiglio di Amministrazione nel suo complesso.

L'autonomia e l'indipendenza dell'OdV sono inoltre garantite dall'autonomia nello stabilire le proprie regole di funzionamento mediante l'adozione di un proprio Regolamento.

L'OdV dispone di autonomi poteri di spesa sulla base di un budget annuale, approvato dal Consiglio di Amministrazione, su proposta dell'OdV stesso. In ogni caso, quest'ultimo può richiedere un'integrazione del budget assegnato, qualora non sufficiente all'efficace espletamento delle proprie incombenze, e può estendere la propria autonomia di spesa di propria iniziativa in presenza di situazioni eccezionali o urgenti, che saranno oggetto di successiva relazione al Consiglio di Amministrazione.

All'OdV e alla funzione della quale esso si avvale sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli, l'OdV deve altresì godere di garanzie tali da impedire che esso stesso o uno dei suoi componenti possano essere rimossi o penalizzati in conseguenza dell'espletamento dei loro compiti.

Nell'esercizio delle loro funzioni i membri dell'OdV non devono trovarsi in situazioni, anche potenziali, di conflitto di interesse con Quaestio, Quaestio Holding S.A. e le società in cui Quaestio Holding S.A. detiene una partecipazione, derivanti da qualsivoglia ragione (ad esempio di natura personale o familiare).

In tali ipotesi essi sono tenuti ad informare immediatamente gli altri membri dell'OdV e devono astenersi dal partecipare alle relative deliberazioni.

Professionalità

L'OdV deve essere composto da soggetti dotati di adeguata esperienza aziendale e delle cognizioni tecniche e giuridiche necessarie per svolgere efficacemente le attività proprie dell'Organismo.

In particolare i componenti dell'OdV devono possedere una consistente esperienza aziendale, maturata all'interno di Quaestio ovvero in società con connotazioni simili per quanto attiene l'attività svolta.

L'OdV può essere coadiuvato, nell'ambito delle proprie attività di vigilanza, dalle Funzioni della Società, per gli ambiti di rispettiva competenza.

Ove necessario, l'OdV può avvalersi, con riferimento all'esecuzione delle operazioni tecniche necessarie per lo svolgimento della funzione di controllo, anche di consulenti esterni. In tal caso, i consulenti dovranno sempre riferire i risultati del loro operato all'OdV.

Continuità di azione

L'OdV deve essere in grado di garantire la necessaria continuità nell'esercizio delle proprie funzioni, anche attraverso la programmazione e pianificazione dell'attività e dei controlli, la verbalizzazione delle riunioni e la disciplina dei flussi informativi provenienti dalle varie aree della SGR.

5.3. Definizione dei compiti e dei poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza è affidato il compito di:

- vigilare sul funzionamento del Modello sia rispetto alla prevenzione della commissione dei reati richiamati dal Decreto, sia con riferimento alla capacità di far emergere il concretizzarsi di eventuali comportamenti illeciti;
- svolgere periodica attività ispettiva e di controllo, di carattere continuativo – con frequenza temporale e modalità predeterminata dal piano delle attività di vigilanza – e controlli a sorpresa, in considerazione dei vari settori di intervento o delle tipologie di attività e dei loro punti critici al fine di verificare l'efficienza ed efficacia del Modello;
- accedere liberamente presso qualsiasi area e unità della Società – senza necessità di alcun consenso preventivo – per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei compiti previsti dal Decreto, da tutti i Destinatari. Nel caso in cui venga opposto un motivato diniego all'accesso agli atti, l'Organismo redige, qualora non concordi con la motivazione opposta, un rapporto da trasmettere al Consiglio di Amministrazione;
- richiedere informazioni rilevanti o l'esibizione di documenti, anche informatici, pertinenti alle attività di rischio, ai Destinatari. In relazione ai soggetti esterni, l'obbligo di questi ultimi di ottemperare alla richiesta dell'Organismo deve essere inserito nei singoli contratti;
- promuovere il costante aggiornamento del Modello, formulando, ove necessario, all'organo dirigente le proposte per eventuali aggiornamenti e adeguamenti da realizzarsi mediante le modifiche e/o le integrazioni che si dovessero rendere necessarie in conseguenza di: i) significative violazioni delle prescrizioni del Modello; ii) significative modificazioni dell'assetto interno di Quaestio e/o delle modalità di svolgimento delle attività d'impresa; iii) modifiche normative;
- verificare il rispetto delle procedure previste dal Modello e rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni e procedere secondo quanto disposto nel Modello;
- assicurare il periodico aggiornamento del sistema di identificazione delle aree sensibili, mappatura e classificazione delle attività sensibili;
- curare i rapporti e assicurare i flussi informativi di competenza verso il Consiglio di Amministrazione, nonché verso il Collegio Sindacale;
- promuovere interventi di comunicazione e formazione sui contenuti del Decreto e del Modello, sugli impatti della normativa sull'attività della SGR e sulle norme comportamentali, instaurando anche dei controlli sulla frequenza;
- verificare la predisposizione di un efficace sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del Decreto garantendo la tutela e riservatezza del segnalante;
- assicurare la conoscenza delle condotte che devono essere segnalate e delle modalità di effettuazione delle segnalazioni;
- fornire chiarimenti in merito al significato ed all'applicazione delle previsioni contenute nel Modello;

- formulare e sottoporre all'approvazione dell'organo dirigente la previsione di spesa necessaria al corretto svolgimento dei compiti assegnati, con assoluta indipendenza. Tale previsione di spesa, che dovrà garantire il pieno e corretto svolgimento della propria attività, deve essere approvata dal Consiglio di Amministrazione. L'Organismo può autonomamente impegnare risorse che eccedono i propri poteri di spesa, qualora l'impiego di tali risorse sia necessario per fronteggiare situazioni eccezionali e urgenti. In questi casi l'Organismo deve informare il Consiglio di Amministrazione nella riunione immediatamente successiva;
- segnalare tempestivamente all'organo dirigente, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;
- promuovere l'attivazione di eventuali procedimenti disciplinari e proporre le eventuali sanzioni;
- verificare e valutare l'idoneità del sistema disciplinare ai sensi e per gli effetti del Decreto.

Nello svolgimento delle predette attività, l'OdV può avvalersi del supporto di altre funzioni interne della SGR e di consulenti esterni con specifiche competenze, il cui apporto professionale si renda di volta in volta necessario, senza necessità di ottenere specifiche autorizzazioni da parte del vertice societario. Anche a tale fine, l'Organismo di Vigilanza viene dotato dal Consiglio di Amministrazione di un budget idoneo allo svolgimento dei compiti ad esso demandati. Detto budget può essere dall'OdV utilizzato a discrezione dello stesso (ad esempio, per l'effettuazione di verifiche che richiedano il ricorso a professionalità esterne alla Società) senza necessità di previa autorizzazione.

Il Consiglio di Amministrazione cura l'adeguata comunicazione alle strutture aziendali del Modello, dei compiti dell'OdV e dei suoi poteri.

I componenti dell'OdV, nonché i soggetti dei quali l'OdV stesso, a qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni (fatte salve le attività di reporting al Consiglio di Amministrazione).

I componenti dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello. I componenti dell'Organismo di Vigilanza si astengono dal ricevere e utilizzare informazioni riservate per fini diversi da quelli compresi nel presente paragrafo, e comunque per scopi non conformi alle funzioni proprie dell'Organismo di Vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

Ogni informazione in possesso dei componenti dell'Organismo di Vigilanza deve essere comunque trattata in conformità con la vigente legislazione in materia e, in particolare, in conformità al Regolamento (UE) 2016/679 ("GDPR) ed al D.lgs. 196/2003 ("Codice Privacy") e successivi aggiornamenti.

Ogni informazione, segnalazione, report, relazione previsti nel Modello sono conservati dall'OdV in un apposito archivio (informatico e/o cartaceo).

5.4. Reporting dell'Organismo di Vigilanza

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'OdV si relaziona direttamente al Consiglio di Amministrazione della SGR e al Comitato Controlli Interni e Rischi.

L'OdV riferisce al Consiglio di Amministrazione e al Collegio Sindacale almeno annualmente in merito alle seguenti tematiche:

- esiti dell'attività di vigilanza espletata nel periodo di riferimento, con l'indicazione di eventuali problematiche o criticità emerse e degli interventi opportuni sul Modello;
- eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno di Quaestio e/o delle modalità di svolgimento delle attività, che richiedono aggiornamenti del Modello (tale segnalazione ha luogo qualora non si sia previamente proceduto a sottoporla al Consiglio di Amministrazione al di fuori della relazione annuale);
- resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del Modello e dei protocolli, nonché all'esito delle conseguenti verifiche effettuate;
- provvedimenti disciplinari e sanzioni eventualmente applicate da Quaestio, con riferimento alle violazioni delle previsioni del Modello e dei protocolli;
- rendiconto delle spese sostenute;
- attività pianificate a cui non si è potuto procedere per giustificate ragioni di tempo e risorse;
- piano delle verifiche predisposto per l'anno successivo.

L'OdV potrà in ogni momento chiedere di essere sentito dal Consiglio di Amministrazione ovvero dal Collegio Sindacale qualora accerti fatti di particolare rilevanza, ovvero ritenga opportuno un esame o un intervento in materie inerenti al funzionamento e all'efficace attuazione del Modello.

A garanzia di un corretto ed efficace flusso informativo, l'OdV ha inoltre la possibilità, al fine di un pieno e corretto esercizio dei propri poteri, di chiedere chiarimenti o informazioni direttamente all'Amministratore Delegato.

L'OdV può, a sua volta, essere convocato in ogni momento dal Consiglio di Amministrazione per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello.

5.5. Flussi informativi nei confronti dell'Organismo di Vigilanza

5.5.1. Flussi informativi a evento

I flussi informativi hanno a oggetto tutte le informazioni e tutti i documenti che devono essere portati a conoscenza dell'OdV, secondo quanto previsto dal Modello, dai protocolli di decisione e dalle policy e regolamenti aziendali, che ne costituiscono parte integrante. Sono stati istituiti in proposito obblighi di comunicazione gravanti, in generale, sui Destinatari del Modello. I flussi ad evento riguardano quanto meno quelli elencati, fermo restando la possibilità dell'OdV di richiederne ulteriori per approfondimenti che ritiene necessario.

In particolare, i responsabili delle aree della SGR che svolgono attività sensibili in accordo con le rispettive attribuzioni organizzative, devono comunicare all'OdV con la necessaria tempestività e in forma scritta, ogni informazione riguardante:

- eventuali documenti di reporting predisposti dalle aree e/o Organi di Controllo (compresa la società di revisione) nell'ambito delle rispettive attività di verifica, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto e/o delle previsioni del Modello e dei protocolli di decisione;
- le indagini disciplinari avviate per presunte violazioni del Modello. Successivamente, a esito delle indagini, evidenza dei provvedimenti disciplinari eventualmente applicati ovvero dei provvedimenti di archiviazione e delle relative motivazioni;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal Decreto e che possano coinvolgere Quaestio;
- notizie:
  - dello svolgimento di procedimenti giudiziari aventi a oggetto la responsabilità amministrativa degli enti *ex* D.lgs. 231/01 in cui sia coinvolta la Società e, alla loro conclusione, i relativi esiti;
  - di eventuali sentenze di condanna di dipendenti di Quaestio a seguito del compimento di reati rientranti tra quelli presupposto del Decreto;
  - di lamentele degli investitori;
- notizie dell'avvio di visite, ispezioni e accertamenti da parte degli enti competenti (quali, ad esempio, Guardia di Finanza, Agenzia delle Entrate, ASL, INPS, INAIL) o da parte di Autorità di Vigilanza e, alla loro conclusione, i relativi esiti;
- eventuali prescrizioni impartite dagli organi ispettivi in materia di igiene e sicurezza sul lavoro nonché ogni altro provvedimento significativo proveniente da Enti Pubblici aventi compiti in materia di salute e sicurezza sul lavoro o dall'Autorità Giudiziaria;
- segnalazioni di incidenti/infortuni, anche derivanti da fattori esterni, che hanno comportato lesioni gravi o gravissime a dipendenti e/o a terzi;

- informativa su azioni criminose tentate o svolte da qualsiasi dipendente o collaboratore e su procedimenti disciplinari svolti ed eventuali sanzioni irrogate relativamente alla violazione del Modello 231;
- informativa su azioni criminose tentate o consumate da terzi;
- variazioni intervenute nel sistema dei poteri e delle deleghe della Società con impatti rilevanti ai fini del Risk Assessment e del Modello di Quaestio (a titolo esemplificativo, le variazioni devono intendersi rilevanti ai fini del flusso in oggetto laddove interessino deleghe di poteri e/o procure che costituiscono livelli autorizzativi nell'ambito di attività sensibili/Protocolli);
- richieste di denaro o altra utilità, anche non esplicite da parte di un Pubblico Ufficiale o Incaricato di Pubblico Servizio, oppure comportamenti scorretti o illegali posti in essere da parte degli stessi;
- variazioni intervenute nella struttura organizzativa con impatti rilevanti ai fini del Risk Assessment e del Modello di Quaestio (a titolo esemplificativo, le variazioni devono intendersi rilevanti ai fini del flusso in oggetto laddove interessino aree della SGR in relazione all'operatività delle quali sono state individuate attività sensibili in fase di Risk Assessment);
- eventuali contenziosi passivi con l'amministrazione finanziaria (ad es. quelli derivanti da accertamenti fiscali);
- richieste di denaro o altra utilità da parte di controparti commerciali per porre in essere comportamenti contrari ai obblighi. Comportamenti scorretti o illegali da parte di controparti commerciali.

L'Organismo di Vigilanza è destinatario anche delle segnalazioni aventi a oggetto il funzionamento e l'aggiornamento del Modello, ossia l'adeguatezza dei principi del Codice Etico e di Comportamento e delle procedure aziendali, nonché della loro applicazione. Più in particolare, tale attività di reporting ha lo scopo di segnalare all'Organismo di Vigilanza l'eventuale esistenza di attività aziendali risultate e/o percepite come prive in tutto o in parte di apposita e/o adeguata regolamentazione. In particolare, l'attività di reporting avrà ad oggetto:

- le carenze della regolamentazione: si parla di carenze nel caso di assenza totale o parziale di specifica regolamentazione;
- il malfunzionamento della regolamentazione esistente: si parla di malfunzionamento in presenza di concreta inadeguatezza dei principi del Codice Etico e/o delle procedure operative rispetto alle finalità cui sono preordinati. Tale circostanza rileva soprattutto nei casi di rilevata e/o percepita carenza della regolamentazione sotto il profilo della chiarezza e comprensibilità, aggiornamento e corretta comunicazione. Tale inadeguatezza può sfociare nella non corretta applicazione della disciplina o nella sua totale o parziale disapplicazione;
- suggerimenti/integrazioni da apportare alla regolamentazione, ossia alle procedure operative e/o ai principi del Codice Etico;
- altre eventuali osservazioni.

Tutti i Destinatari del Modello devono inoltre segnalare tempestivamente all'OdV gli eventi di seguito riportati dei quali vengano direttamente o indirettamente a conoscenza:

- la commissione, la presunta commissione o il ragionevole pericolo di commissione di reati o illeciti previsti dal Decreto;
- la violazione o le presunte violazioni del Modello o dei protocolli di decisione;
- ogni fatto/comportamento/situazione con profili di criticità e che potrebbe esporre Quaestio alle sanzioni di cui al Decreto.

L'obbligo di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello e nei protocolli di decisione rientra nel più ampio dovere di diligenza e obbligo di fedeltà del prestatore di lavoro.

Il corretto adempimento dell'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari. In particolare, Quaestio garantisce:

- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Le informazioni di cui sopra possono essere segnalate, anche in forma anonima, e pervenire all'OdV tramite una delle seguenti modalità:

A) nel caso dei componenti degli Organi Sociali, di tutti i dipendenti e di coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale della SGR, anche in forma diversa dal rapporto di lavoro subordinato (il "Personale"), essi sono tenuti ad effetturare segnalazioni secondo le modalità descrittte nella Policy A.02 "Policy in materia di Whistleblowing".

A tal riguardo il Responsabile per il Ricevimento, Esame e Valutazione delle Segnalazioni non appena ricevuta la segnalazione provvede a informare l'Organismo di Vigilanza, il Presidente del Collegio Sindacale, il Presidente del Consiglio di Amministrazione e il Presidente del CCIR, tenendoli informati anche circa le conclusioni a cui si è giunti ad esito delle verifiche effettuate.

Nel caso di segnalazioni di condotte illecite rilevanti ai sensi del Modello di Organizzazione, Gestione e Controllo ex D.Lgs 231/2001 della SGR, il Responsabile per il Ricevimento, Esame e Valutazione delle Segnalazioni dovrà coordinare le proprie attività con l'Organismo di Vigilanza ex D.Lgs 231/2001 della SGR e, nel caso ne venga richiesto, dovrà collaborare con lo stesso per l'approfondimento di tali segnalazioni.

Al termine dell'indagine, il Responsabile dei sistemi interni di segnalazione predispone una relazione all'interno della quale sono riportate:

- l'iter dell'indagine e la documentazione raccolta;
- le conclusioni alle quali si è giunti;
- le raccomandazioni e le azioni da porre in essere per sopperire alle violazioni riscontrate e assicurare che queste non si verifichino in futuro.

Tale relazione è inviata per conoscenza ai soggetti con i quali è stata condivisa la segnalazione così come riportati nel paragrafi precedenti.

B) nel caso di destinari diversi di quelli di cui al punto A), essi possono effetturare segnalazioni attraverso:

- posta cartacea, anche in forma anonima, al seguente indirizzo:

  Quaestio Capital Management Società di Gestione del Risparmio S.p.A.

  C/A Organismo di Vigilanza ex D.lgs. 231/2001

  Corso Como, 15

  20154 Milano

L'Organismo di Vigilanza valuta tutte le segnalazioni ricevute secondo le modalità di cui ai precedenti punti A) e B), purché presentino elementi fattuali, ossia tali da risultare sufficientemente circostanziati e verificabili, e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere a una indagine interna. L'OdV può dare luogo a tutti gli accertamenti e le indagini che ritenga necessarie ad appurare il fatto segnalato. Le determinazioni dell'OdV in ordine all'esito dell'accertamento devono essere motivate per iscritto.

La legge n. 179, 30 novembre 2017, recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", successivamente abrogata dal Decreto Legislativo n. 24 del 10 marzo 2023 , attuativo della Direttiva UE 2019/1937, ha introdotto il sistema del c.d. "Whistleblowing", volto alla tutela del dipendente o collaboratore che segnali illeciti. Pertanto, l'Organismo di Vigilanza assicurerà la riservatezza e delle informazioni di cui entri in possesso, nonché delle relative fonti. Da parte sua la Società garantisce la tutela dei segnalanti e non effettuerà alcuna azione classificabile come ritorsiva (sanzione disciplinare, demansionamento, sospensione, licenziamento) o discriminatoria, nei confronti del personale che abbia riferito, in buona fede, eventi o situazioni tali da far presumere che si potesse essere verificata una violazione del Modello, del Codice Etico e di Comportamento, dei protocolli diretti a programmare l'attuazione delle decisioni della Società in relazione ai reati

da prevenire o della normativa in materia di responsabilità amministrativa delle Società. La Società assicura la riservatezza e l'anonimato del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente ed in mala fede.

Ogni informazione e segnalazione prevista nel Modello è conservata dall'OdV in un apposito archivio informatico e/o cartaceo per un periodo di dieci anni, in conformità alle disposizioni contenute nel D.lgs. 196/2003 e nel Regolamento (UE) 2016/679, in materia di protezione dei dati personali.

Oltre agli obblighi di segnalazione di cui sopra, l'Amministratore Delegato, ovvero i responsabili delle aree della SGR, nell'ambito delle responsabilità agli stessi attribuite, sono tenuti a comunicare all'OdV ogni informazione rilevante per il rispetto, il funzionamento e l'adeguamento del presente Modello.

L'eventuale omessa o ritardata comunicazione all'OdV dei flussi informativi sopra elencati sarà considerata violazione del Modello e potrà essere sanzionata secondo quanto previsto dal sistema disciplinare di cui al successivo capitolo.

I suddetti obblighi informativi a carico dei Destinatari del Modello, si aggiungono ai più ampi obblighi previsti dalla normativa interna adottata dalla SGR in materia di segnalazione di "comportamenti illegittimi".

5.5.2. Flussi informativi periodici

L'Organismo di Vigilanza esercita le proprie responsabilità di controllo anche mediante l'analisi di sistematici flussi informativi periodici trasmessi dalle funzioni Internal Audit, dall'Area controlli, dall'area Amministrazione e Controllo, dall'area HR, dal Datore di Lavoro ai sensi del D.lgs. 81/2008, nonché dai responsabili delle aree della SGR. In particolare:

- le funzioni Internal Audit, il Chief Risk Officer, la Funzione AML/SOS e la Funzione Compliance trasmettono, con cadenza almeno annuale, relazioni contenenti un'informativa circa le verifiche svolte, le principali risultanze, le azioni riparatrici pianificate e il relativo stato di realizzazione, gli ulteriori interventi di controllo in programma nel semestre successivo, in linea con i piani annuali delle funzioni. Laddove ne ravvisi la necessità, l'Organismo di Vigilanza richiede alla funzione copia dei report di dettaglio per i punti specifici che ritiene di voler meglio approfondire; in particolare nella relazione di compliance sono contenuti riferimenti alle variazioni nei processi e nelle procedure, nonché lo stato di allineamento del sistema dei poteri e delle deleghe;
- il Datore di Lavoro trasmette (i) una relazione annuale contenente l'esito delle attività svolte in relazione all'organizzazione e al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza nei luoghi di lavoro e (ii) il verbale della "riunione periodica" sulla sicurezza tra il Datore di Lavoro (o un suo delegato), il Responsabile del Sistema di Prevenzione e Protezione, il Medico Competente e il Responsabile dei Lavoratori per la Sicurezza, prevista dall'art. 35 del D.lgs. 81/2008;

- il Chief Risk Officer tramette annualmente, la Relazione sulla Struttura Organizzativa della SGR dando evidenza delle principali variazioni intervenute nella struttura organizzativa;
- la funzione HR trasmette un flusso di rendicontazione con cadenza semestrale concernente i provvedimenti disciplinari eventualmente comminati al personale dipendente nel periodo di riferimento;

la funzione Amministrazione e Controllo tramette un flusso di rendicontazione con cadenza semestrale concernentel'elenco dei contenziosi attivi e passivi in corso quando la controparte sia un Ente o un Soggetto Pubblico o equiparato e, alla loro conclusione, i relativi esiti.

Oltre ai flussi informativi a evento e periodici sopra rappresentati, l'Organismo di Vigilanza potrà richiedere, tempo per tempo, ulteriori flussi informativi a supporto delle proprie attività di vigilanza sul funzionamento e l'osservanza del Modello e di cura dell'aggiornamento dello stesso, definendo le relative modalità e tempistiche di trasmissione.

È facoltà comunque dell'OdV proporre le variazioni ritenute necessarie ai flussi informativi sopra rappresentati.

6. SISTEMA DISCIPLINARE

Il presente capitolo definisce il sistema disciplinare/sanzionatorio inerente esclusivamente alle violazioni delle regole e dei principi di controllo e di comportamento definiti nel Modello di organizzazione, gestione e controllo ex D.lgs. 231/2001, fatte salve le sanzioni previste dalla SGR per altre tipologie di infrazioni.

6.1. Principi generali

L'art. 6, commi 2, lett. e) e 2-bis, lett. d) e l'art. 7, comma 4, lett. b) del Decreto indicano, quale condizione per un'efficace attuazione del modello di organizzazione, gestione e controllo, l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello stesso.

Pertanto, l'adozione di un adeguato sistema disciplinare che sanzioni le violazioni dei principi contenuti nel presente Modello rappresenta un requisito imprescindibile per una piena ed efficace attuazione del Modello stesso.

La definizione di uno specifico sistema di sanzioni, oltre a prevenire la commissione di infrazioni, consente all'OdV di esercitare la funzione di vigilanza con maggiore efficienza e garantisce l'effettiva osservanza del Modello stesso.

Il sistema disciplinare è diretto a sanzionare il mancato rispetto da parte dei Destinatari dei principi e delle regole di condotta prescritti nel presente Modello (e nei documenti che ne costituiscono parte integrante).

Su tale presupposto, la SGR adotterà nei confronti:

- del personale dipendente, il sistema disciplinare adottato dalla SGR e dalle leggi che regolano la materia;
- di tutti i soggetti esterni, i provvedimenti stabiliti dalle disposizioni contrattuali e di legge che regolano la materia.

L'attivazione, sulla base delle segnalazioni pervenute dall'Organismo di Vigilanza, lo svolgimento e la definizione del procedimento disciplinare nei confronti dei dipendenti, a seguito di riscontrate violazioni del presente Modello, sono affidati all'Amministratore Delegato che si avvale del supporto dell'unità Personale. Il procedimento disciplinare nei confronti del personale dirigente è di competenza del Consiglio di Amministrazione.

Gli interventi sanzionatori nei confronti dei soggetti esterni sono affidati alla funzione che gestisce il contratto o presso cui opera il lavoratore autonomo ovvero il fornitore.

Le sanzioni sono commisurate al livello di responsabilità e autonomia operativa del lavoratore, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità e gravità della condotta, ovvero a tutte le altre particolari circostanze che possono aver caratterizzato la violazione del Modello. Le sanzioni sono applicate in conformità all'art. 7 della Legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori), al CCNL vigente all'interno della SGR, nonché al sistema disciplinare della stessa.

Pertanto, nel deliberare sulla sanzione applicabile al caso concreto, la SGR deve considerare la tipologia di rapporto di lavoro instaurato con il prestatore (subordinato dirigenziale e non dirigenziale), la specifica disciplina legislativa e contrattuale, nonché i seguenti criteri:

- gravità della violazione;
- tipologia dell'illecito perpetrato;
- circostanza in cui si sono svolti i comportamenti illeciti;
- eventualità che i comportamenti integrino esclusivamente un tentativo di violazione;
- eventuale recidività del soggetto.

L'Organismo di Vigilanza, nell'ambito dei compiti allo stesso attribuiti, monitora costantemente i procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché gli interventi nei confronti dei soggetti esterni.

In applicazione dei suddetti criteri, viene stabilito il seguente sistema sanzionatorio.

6.2. Provvedimenti per inosservanza da parte dei dipendenti

6.2.1. Aree professionali e quadri direttivi

Al personale appartenente alle aree professionali e ai quadri direttivi sono applicabili i seguenti provvedimenti:

- richiamo verbale, in caso di lieve inosservanza delle norme di comportamento del Codice Etico e di Comportamento, del presente Modello, delle policy e procedure aziendali e del Sistema dei Controlli Interni che non abbiano generato rischi o sanzioni per la SGR;
- ammonizione scritta, in caso di inosservanza colposa delle norme di comportamento del Codice Etico e di Comportamento, del presente Modello, delle policy e procedure aziendali e del Sistema dei Controlli Interni, oltre al mancato adempimento alle richieste di informazioni o di esibizione di documenti da parte dell'OdV;
- multa in misura non eccedente l'importo di quattro ore della normale retribuzione, in caso di mancanze punibili con le precedenti sanzioni, quando per circostanze obiettive, per conseguenze specifiche o per recidività, rivestano maggiore importanza;
- sospensione della retribuzione e dal servizio per un massimo di cinque giorni, nei casi di inosservanza ripetuta o grave delle norme di comportamento del Codice Etico e di Comportamento, del presente Modello, delle policy e procedure aziendali e del Sistema dei Controlli Interni, oltre al ripetuto inadempimento alle richieste di informazioni o di esibizione di documenti da parte dell'OdV;

- sospensione dal servizio con mantenimento del trattamento economico per lavoratori sottoposti a procedimento penale ex D.lgs. 231/2001 per motivi cautelari;
- licenziamento per mancanze, in caso di violazione dolosa o con colpa grave delle norme di comportamento del Codice Etico e di Comportamento, del presente Modello, delle policy e procedure aziendali e del Sistema dei Controlli Interni tali da provocare un grave danno morale o materiale a Quaestio.

6.2.2. Personale dirigente

Il rapporto dirigenziale si caratterizza per la natura eminentemente fiduciaria. Il comportamento del dirigente oltre a riflettersi all'interno della SGR, costituendo modello ed esempio per tutti coloro che vi operano, si ripercuote anche sull'immagine esterna della medesima. Pertanto, il rispetto da parte dei dirigenti della SGR delle prescrizioni del Modello, del Codice Etico e di Comportamento, e delle relative procedure di attuazione costituisce elemento essenziale del rapporto di lavoro dirigenziale.

Nei confronti dei dirigenti che abbiano commesso una violazione del Modello, del Codice Etico e di Comportamento o delle procedure stabilite in attuazione del medesimo, il Consiglio di Amministrazione, eventualmente con il supporto dell'unità Personale, avvia i procedimenti di competenza per effettuare le relative contestazioni e applicare le misure sanzionatorie più idonee, in conformità con quanto previsto dal CCNL applicabile ai dirigenti vigente e, ove necessario, con l'osservanza delle procedure di cui all'art. 7 della Legge 30 maggio 1970, n. 300.

Le sanzioni devono essere applicate nel rispetto dei principi di gradualità e proporzionalità rispetto alla gravità del fatto e della colpa o dell'eventuale dolo. Tra l'altro, con la contestazione può essere disposta cautelativamente la revoca delle eventuali procure affidate al soggetto interessato, fino alla eventuale risoluzione del rapporto in presenza di violazioni così gravi da far venir meno il rapporto fiduciario con la SGR.

6.3. Provvedimenti per inosservanza da parte dei componenti del Consiglio di Amministrazione e del Collegio Sindacale

In caso di violazione del Modello da parte dei componenti del Consiglio di Amministrazione o del Collegio Sindacale, l'OdV deve informare, mediante relazione scritta, i membri non coinvolti del Consiglio di Amministrazione e del Collegio Sindacale i quali prenderanno gli opportuni provvedimenti. Nei confronti dei componenti del Consiglio di Amministrazione o del Collegio Sindacale che abbiano commesso una violazione del Modello, può essere applicato ogni idoneo provvedimento consentito dalla legge.

Nel caso in cui uno degli Amministratori o Sindaci coinvolti coincida con il Presidente del Consiglio di Amministrazione o del Collegio Sindacale, si rinvia a quanto previsto dalla legge in tema di urgente convocazione dell'Assemblea dei Soci.

6.4. Provvedimenti per inosservanza da parte dei soggetti esterni destinatari del Modello

Ogni comportamento in violazione del Modello o che sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto, posto in essere dai soggetti esterni, come definiti nel presente Modello, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata del rapporto contrattuale per giusta causa, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti alla SGR. Anche a tale scopo, la Società, nella regolazione contrattuale dei rapporti con le controparti, si riserva tramite apposita previsione la facoltà di risolvere gli stessi in caso di violazioni rilevanti.

7. INFORMAZIONE E FORMAZIONE DEL PERSONALE

7.1. Diffusione del Modello

Le modalità di comunicazione del Modello devono essere tali da garantirne la piena pubblicità, al fine di assicurare che i destinatari siano a conoscenza delle procedure che devono seguire per adempiere correttamente alle proprie mansioni.

L'informazione deve essere completa, tempestiva, accurata, accessibile e continua.

A tal fine è previsto l'accesso diretto a un'apposita cartella della rete aziendale condivisa sulla *repository* sharepoint, nella quale è disponibile e costantemente aggiornata tutta la documentazione di riferimento in materia di D.lgs. 231/2001. Ai soggetti che avviano un rapporto di collaborazione con la SGR (i neo-assunti) viene tempestivamente fornito accesso a detta cartella, sollecitando gli stessi all'attenta lettura del contenuto della stessa.

L'attività di comunicazione e formazione è supervisionata dall'OdV, avvalendosi delle aree competenti, alle quali è assegnato il compito di promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, dei contenuti del Decreto, degli impatti della normativa sull'attività di Quaestio, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello e di promuovere e coordinare le iniziative volte ad agevolare la conoscenza e la comprensione del Modello da parte di tutti coloro che operano per conto della SGR.

7.2. Formazione del personale

Ai fini dell'efficace attuazione del Modello, è obiettivo generale della SGR garantire a tutti i Destinatari del Modello la conoscenza dei principi e delle disposizioni in esso contenuti.

Quaestio persegue, attraverso un adeguato programma di formazione aggiornato periodicamente e rivolto a tutti i dipendenti, una loro sensibilizzazione continua sulle problematiche attinenti al Modello, al fine di raggiungere la piena consapevolezza delle direttive aziendali e di essere posti in condizioni di rispettarle in pieno.

Al fine di garantire un'efficace attività di formazione, la SGR promuove e agevola la conoscenza dei contenuti del Modello da parte dei dipendenti, con grado di approfondimento diversificato a seconda del loro coinvolgimento nelle attività individuate come sensibili ai sensi del Decreto.

Gli interventi formativi, che potranno essere erogati sia in modalità e-learning che in aula hanno ad oggetto:

- una parte generale, indirizzata a tutti i dipendenti, volta a illustrare il quadro normativo di riferimento della responsabilità amministrativa degli Enti e i contenuti generali del Modello;
- una parte specifica, differenziata per aree di attività dei dipendenti, diretta a illustrare le attività individuate come sensibili ai sensi del Decreto e i relativi protocolli contenuti nella parte speciale del Modello;

- una verifica del grado di apprendimento della formazione ricevuta.

I contenuti formativi sono opportunamente aggiornati in relazione all'evoluzione del contesto normativo e del Modello.

La partecipazione ai corsi formativi è obbligatoria e deve essere documentata attraverso la richiesta della firma di presenza. L'OdV, per il tramite delle preposte aree aziendali, raccoglie e archivia le evidenze relative all'effettiva partecipazione ai suddetti interventi formativi.

Periodicamente, in coerenza con l'evoluzione della normativa di riferimento e con le modifiche della struttura organizzativa aziendale, si procede alla reiterazione dei corsi, al fine di verificare l'effettiva applicazione del Modello da parte dei Destinatari nonché la loro sensibilizzazione alle prescrizioni dello stesso, secondo modalità indicate dall'OdV al Consiglio di Amministrazione, in coordinamento con le aree aziendali competenti.

A ogni modo, è compito dell'OdV valutare l'efficacia del piano formativo con riferimento al contenuto dei corsi, alle modalità di erogazione, alla loro reiterazione, ai controlli sull'obbligatorietà della frequenza e alle misure adottate nei confronti di quanti non li frequentino senza giustificato motivo.

8. AGGIORNAMENTO DEL MODELLO

L'adozione e l'efficace attuazione del Modello costituiscono per espressa previsione legislativa una responsabilità del Consiglio di Amministrazione. L'efficacia del Modello è garantita dalla costante attività di aggiornamento, intesa sia come integrazione sia come modifica delle parti che costituiscono lo stesso.

A titolo esemplificativo, l'aggiornamento del Modello può rendersi necessario in presenza delle seguenti circostanze:

- aggiornamento o modifica del catalogo dei reati presupposto;
- evoluzioni normative e giurisprudenziali;
- modifiche relative alla struttura organizzativa e alle aree di business.

Il potere di aggiornare il Modello compete:

- al Consiglio di Amministrazione per modifiche sostanziali, quali, ad esempio, l'aggiornamento o modifica delle aree sensibili in considerazione di evoluzioni normative (ad esempio, introduzione nel Decreto di nuovi reati presupposto) o di mutamenti del business (ad esempio, introduzione di nuovi ambiti di operatività), l'approvazione e modifica dei Protocolli;
- all'Amministratore Delegato, su specifica delega del Consiglio di Amministrazione, per le modifiche non sostanziali del Modello e dei Protocolli, ovvero per quelle dovute a riorganizzazioni e conseguente riassegnazione a diverse strutture organizzative di attività a rischio-reato già individuate e non variate nella sostanza, o per modifiche di carattere formale (ridenominazione di attività/aree/unità della SGR).

PARTE SPECIALE

9. METODOLOGIA DI INDIVIDUAZIONE DELLE AREE SENSIBILI

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

Pertanto, sono state identificate le attività a rischio di commissione dei reati rilevanti ai sensi del Decreto e quelle strumentali, intendendosi rispettivamente le attività il cui svolgimento può dare direttamente adito alla commissione di una delle fattispecie di reato contemplate dal decreto e le attività in cui, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei reati (in generale "Attività sensibili").

Nella Parte Speciale del Modello, le attività sensibili individuate in fase di risk assessment (attività a rischio-reato) sono distribuite in "Aree Sensibili", ciascuna delle quali concerne una o più "famiglie di reato" e/o fattispecie di reato, individuate per comunanza di attività sensibili e "principi di controllo" e "principi di comportamento" aventi efficacia ai fini del presidio dei rischi di commissione dei reati presupposto del Decreto.

9.1. Identificazione dei Reati e delle operazioni a rischio

Nell'ambito delle attività e della complessiva operatività aziendale della Società, sono individuate, per tipologia di reato, le seguenti attività sensibili.

9.1.1. Reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto), reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità di giudiziaria (art. 25-*decies* del Decreto), reati di corruzione tra privati e di istigazione alla corruzione tra privati (art. 25-*ter* del Decreto)

Ai sensi dell'art. 6 del Decreto, nell'ambito delle attività che implichino rapporti con pubblici ufficiali, incaricati di pubblico servizio, autorità di vigilanza o di controllo, organismi ispettivi, enti pubblici erogatori di contributi e finanziamenti agevolati, enti pubblici e soggetti incaricati di pubblico servizio titolari di poteri autorizzativi, concessori, abilitativi, certificativi o regolatori sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui agli artt. 24, 25 e 25-*decies* del Decreto:

- Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni;
- Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- Gestione dei procedimenti autorizzativi legati all'attività istituzionale con le Autorità di Vigilanza;
- Gestione del sistema informativo della Società;

- Gestione degli adempimenti fiscali e delle relazioni con gli Enti Pubblici competenti in materia, anche nel corso di ispezioni;
- Gestione del contenzioso, giudiziale e stragiudiziale;
- Gestione dei rapporti con gli Enti Assistenziali e Previdenziali e altri Enti pubblici e degli adempimenti di legge in materia di lavoro e previdenza;
- Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- Accesso al sistema informatico o database di terzi;
- Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- Gestione dei reclami.

Sono altresì stati individuati i seguenti processi da considerarsi sia come "strumentali" alle attività sopra esaminate in quanto, pur non essendo caratterizzati dall'esistenza di rapporti diretti con la Pubblica Amministrazione, possono costituire supporto e presupposto (finanziario ed operativo) per la commissione dei reati nei rapporti con la P.A., sia come attività "sensibili" con riferimento al reato di corruzione tra privati e di istigazione alla corruzione tra privati di cui agli artt. 2635 e 2635-bis c.c. come richiamati dall'art. 25-ter co. 1° lett. s-bis), in quanto caratterizzati dall'esistenza di rapporti diretti con soggetti privati che esercitino funzioni direttive all'interno di società o enti - privati - oppure che siano amministratori, direttori generali, sindaci, liquidatori, dirigenti preposti alla redazione dei documenti contabili societari all'interno delle medesime società o enti oppure ancora che siano soggetti sottoposti alla direzione o alla vigilanza degli stessi:

- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione dei c/c della SGR;
- Utilizzo delle carte di credito e debito aziendali;
- Gestione del processo di selezione e assunzione del personale;
- Gestione del processo di valutazione, remunerazione e incentivazione del personale;
- Organizzazione delle trasferte;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati;
- Gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti;
- Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali.

9.1.2. Reati informatici e trattamento illecito di dati (art. 24-*bis* del Decreto)

Ai sensi dell'art. 6 del Decreto, nell'ambito delle attività che in generale implichino l'utilizzo diretto o indiretto di sistemi informatici o telematici sono individuate, presso Quaestio, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 24-*bis* del Decreto:

- Gestione del sistema informativo della Società;
- Gestione della sicurezza fisica dei locali, delle relative informazioni e delle apparecchiature;
- Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;
- Accesso al sistema informatico o database di terzi;
- Utilizzo dei meccanismi di firma digitale aziendali;
- Gestione delle caselle di posta elettronica certificata aziendali;
- Archiviazione della documentazione.

9.1.3. Reati di falsità in monete (art. 25-*bis* del Decreto)

Ai sensi dell'art.6 del Decreto, non sono individuate presso la SGR operazioni a rischio.

9.1.4. Reati contro l'industria e il commercio (art. 25-*bis* 1 del Decreto)

Ai sensi dell'art.6 del Decreto, non sono individuate presso la SGR operazioni a rischio.

9.1.5. Reati societari (art. 25-*ter* del Decreto) e Abusi di mercato (art. 25-*sexies* del Decreto)

Ai sensi dell'art. 6 del Decreto, sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*ter* del Decreto e all'art. 25-*sexies* del Decreto:

- Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- Gestione dei procedimenti autorizzativi legati all'attività istituzionale con le Autorità di Vigilanza;
- Gestione degli adempimenti informativi nei confronti di Autorità di Vigilanza;
- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione dei c/c della SGR;
- Utilizzo delle carte di credito e debito aziendali;

- Investimenti e operazioni su strumenti finanziari effettuate dalla SGR;
- Gestione delle operazioni con parti correlate;
- Gestione della contabilità e delle attività funzionali alla predisposizione del bilancio;
- Predisposizione del bilancio di esercizio e dei bilanci intermedi;
- Gestione degli adempimenti fiscali e delle relazioni con gli Enti Pubblici competenti in materia, anche nel corso di ispezioni;
- Gestione del processo di selezione e assunzione del personale;
- Gestione del processo di valutazione, remunerazione e incentivazione del personale;
- Gestione del contenzioso, giudiziale e stragiudiziale;
- Organizzazione delle trasferte;
- Gestione dei rapporti con gli Enti Assistenziali e Previdenziali e altri Enti pubblici e degli adempimenti di legge in materia di lavoro e previdenza;
- Negoziazione contratti e accordi;
- Organizzazione e gestione delle riunioni degli organi sociali e tenuta dei libri sociali;
- Gestione degli adempimenti di segreteria societaria;
- Gestione dei rapporti con il Collegio Sindacale;
- Gestione dei rapporti con la Società di revisione;
- Redazione di documenti, nonché formazione di ogni informazione privilegiata;
- Gestione del sito internet aziendale;
- Utilizzo dei social network;
- Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati;
- Negoziazione delle condizioni economiche dei servizi esecutivi con le controparti;
- Gestione dei rapporti con la Banca Depositaria;
- Gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti;
- Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali;
- Valutazione del portafoglio degli OICR gestiti;
- Gestione dei reclami.

9.1.6. Reati di terrorismo e di eversione dell'ordine democratico (art. 25-*quater* del Decreto)

Ai sensi dell'art. 6 del Decreto, nell'ambito delle attività che implicano il rischio di istaurare rapporti con controparti, clientela o soggetti che si abbia motivo di sospettare che perseguano o agevolino, direttamente o indirettamente, finalità di terrorismo o di eversione dell'ordine costituzionale sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*quarter* del Decreto:

- Gestione degli adempimenti antiriciclaggio e antiterrorismo;
- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati;
- Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali;
- Gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti;
- Negoziazione delle condizioni economiche dei servizi esecutivi con le controparti.

9.1.7. Reati contro la personalità individuale (art. 25-*quinquies* del Decreto) e reati di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies* del Decreto)

Ai sensi dell'art. 6 del Decreto, sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui agli articoli 25-*quinquies* e 25-*duodecies* del Decreto:

- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione del processo di selezione e assunzione del personale;

9.1.8. Reati di criminalità organizzata (art. 24-ter del Decreto), reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies del Decreto) e reati transnazionali e riciclaggio (Legge 16 marzo 2006, n. 146)

Ai sensi dell'art. 6 del Decreto, in riferimento anche al rischio di instaurare rapporti con persone fisiche o giuridiche che si ha motivo di sospettare che perseguano, direttamente o indirettamente, attività illecite che possano rilevare ai sensi dell'art. 24-*bis* e dell'art. 25-*octies* del Decreto, nonché della Legge 146/06, sono individuate, presso la Società, le seguenti operazioni a rischio:

- Gestione degli adempimenti antiriciclaggio e antiterrorismo;
- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione dei c/c della SGR;
- Gestione degli adempimenti fiscali e delle relazioni con gli Enti Pubblici competenti in materia, anche nel corso di ispezioni;
- Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati;
- Gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti;
- Negoziazione delle condizioni economiche dei servizi esecutivi con le controparti;
- Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali.

9.1.9. Reati in materia di salute e sicurezza sul lavoro (art. 25-*septies* del Decreto)

Nell'ambito di tutti i settori di attività della Società e delle sue unità produttive alle quali siano addetti sia lavoratori dipendenti, sia lavoratori dipendenti di imprese esterne o lavoratori autonomi a cui la Società affida i lavori in appalto o in sub-appalto, l'analisi dei processi aziendali della Società ha consentito di individuare, quali *attività* ritenute sensibili

con riferimento ai reati previsti dall'art. 25-*septies* del Decreto, quelle relative alla gestione degli adempimenti in materia di salute e sicurezza nei luoghi lavoro.

9.1.10. Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies*.1 del Decreto)

Ai sensi dell'art. 6 del Decreto, sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*octies*.1 del Decreto:

- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione degli adempimenti antiriciclaggio e antiterrorismo;
- Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali;
- Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, e stipulazione di strumenti derivati non negoziati su mercati regolamentati italiani ed europei;
- Gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti (owner delle Società) con cui sono realizzate le operazioni di investimento e disinvestimento del patrimonio dei Fondi gestiti (a titolo esemplificativo, operazioni di compravendita di quote e azioni di società e di veicoli di investimento non quotate/i);
- Negoziazione delle condizioni economiche dei servizi esecutivi con le controparti;
- Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- ;
- Utilizzo delle carte di credito e di debito aziendali.

9.1.11. Reati in materia di violazione di diritto d'autore (art. 25-*novies* del Decreto)

Ai sensi dell'art. 6 del Decreto, sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*novies* del Decreto:

- Gestione del sistema informativo della Società;
- Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;
- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione del sito internet aziendale;
- Utilizzo dei social network;
- Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società.

9.1.12. Reati ambientali (art. 25-*undecies* del Decreto)

Ai sensi dell'art. 6 del Decreto, sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*undecies* del Decreto:

- gestione dei rifiuti prodotti nell'ambito dell'operatività ordinaria della SGR.

9.1.13. Reati di razzismo e xenofobia (art. 25-*terdecies* del Decreto)

Ai sensi dell'art. 6 del Decreto, non sono individuate presso la SGR operazioni a rischio.

9.1.14. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies* del Decreto)

Ai sensi dell'art. 6 del Decreto, non sono individuate presso la SGR operazioni a rischio.

9.1.15. Reati tributari (art. 25-*quinquiesdecies* del Decreto)

Ai sensi dell'art. 6 del Decreto, sono individuate, presso la Società, le seguenti operazioni a rischio, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*quinquiesdecies* del Decreto:

- Gestione del sistema informativo della Società;
- Gestione del processo di selezione dei fornitori e di outsourcer;
- Gestione delle operazioni con parti correlate;
- Gestione della contabilità e delle attività funzionali alla predisposizione del bilancio;
- Gestione degli adempimenti fiscali e delle relazioni con gli Enti Pubblici competenti in materia, anche nel corso di ispezioni;
- Gestione del processo di valutazione, remunerazione e incentivazione del personale;
- Archiviazione della documentazione.

9.1.16. Reato di contrabbando e diritti di confine (art. 25-*sexdecies* del Decreto)

Ai sensi dell'art. 6 del Decreto, non sono individuate presso la SGR operazioni a rischio.

9.1.17. Delitti contro il patrimonio culturale (art. 25-*septiesdecies* del Decreto), nonché Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies* del Decreto)

Ai sensi dell'art. 6 del Decreto, non sono individuate presso la SGR operazioni a rischio.

10. PRINCIPI GENERALI PER LE PROCEDURE PER LA PREVENZIONE DEI REATI

La Società si impegna a condurre le proprie attività con integrità, correttezza e professionalità, al fine di perseguire le finalità statutarie e la realizzazione della propria mission. Ai Destinatari è pertanto espressamente fatto obbligo, tra l'altro, di:

(i) evitare qualsiasi condotta che possa facilitare o far sorgere il sospetto della commissione di qualsiasi tipo di illecito, minando la fiducia, la trasparenza o la tranquillità dell'ambiente di lavoro e del contesto economico in cui opera;

(ii) manifestare integrità morale nelle azioni intraprese per conto della Società;

(iii) svolgere le attività a favore della Società, in conformità alle norme applicabili e alle disposizioni aziendali applicabili.

I seguenti principi generali informano le procedure che devono essere inderogabilmente osservate ai fini del rispetto del Modello.

Il sistema di organizzazione della Società deve essere, in primo luogo, ispirato al rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale.

Il sistema di organizzazione della Società deve, inoltre, essere fondato sui requisiti fondamentali di chiara, formale e conoscibile descrizione ed individuazione dei compiti e dei poteri attribuiti a ciascuna funzione, alle diverse qualifiche e ruoli professionali; sulla precisa descrizione delle linee di riporto; sulla tracciabilità di ciascun passaggio decisionale e operativo rilevante.

In particolare:

- le responsabilità della gestione (e le relative modalità operative) di una operazione o di un processo aziendale devono essere chiaramente definite e conosciute all'interno della Società;
- deve esservi una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando la Società e manifestando la sua volontà;
- i poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- all'interno di ogni processo aziendale devono essere separate le funzioni e individuati soggetti diversi competenti per la decisione, l'attuazione, la registrazione o il controllo di una operazione. In particolare, deve essere 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; altrettanto, va perseguita una chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio ed in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa.

Inoltre:

- i controlli effettivamente svolti devono essere precisamente documentati in modo che sia possibile identificare chi li ha eseguiti, quando sono stati svolti e con quale esito;
- devono essere previsti meccanismi di sicurezza che garantiscano una adeguata protezione/accesso fisico-logistico ai dati e ai beni aziendali.

10.1. Decisioni dei soggetti apicali e conflitti di interessi

La formazione e l'attuazione delle decisioni degli amministratori sono disciplinate dai principi e dalle prescrizioni contenute nelle disposizioni di legge vigenti, nell'atto costitutivo, nello Statuto, nel Codice Etico e di Comportamento, nel Modello, nel Sistema dei Controlli Interni.

Gli amministratori hanno l'obbligo di comunicare tempestivamente al Consiglio di Amministrazione, al Collegio Sindacale e all'Organismo, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative alle cariche assunte o alle partecipazioni di cui sono titolari, direttamente o indirettamente, in altre società o imprese, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia, possono lasciare ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.

Vi è il medesimo obbligo di comunicazione di cui al punto precedente a carico dei dirigenti che si trovino in posizione apicale, i quali dovranno informare l'Amministratore Delegato e l'Organismo.

Vi è il medesimo obbligo di comunicazione per gli esponenti di Quaestio nominati negli organi sociali di partecipate estere con riferimento all'esistenza di vincoli di parentela o affinità con esponenti della P.A. locale e/o fornitori, clienti o terzi contraenti della Società medesima.

I soggetti interni della Società devono astenersi dal ricevere da terzi qualsiasi utilità avente causa nei ruoli o nelle masioni agi stessi assegnati ovvero che possa indurli a tenere comportamenti in contrasto con gli interessi della Società, degli investitori e dei clienti. Si applicano le disposizioni della policy degli incentivi, le cui violazioni sono da ritenersi tali anche per il presente Modello.

10.2. Comunicazioni all'esterno della società e rapporti con Autorità pubbliche di vigilanza, controllo e Pubblica Amministrazione

Sono tempestivamente e correttamente effettuate, in modo veridico e completo, le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità o Organi di Vigilanza o controllo (italiani, sovranazionali o stranieri), del mercato o dei soci.

È prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste.

La corrispondenza intrattenuta con le Autorità di Vigilanza è formalmente archiviata nella casella di posta elettronica Certificata e presso l'Archivio dell'Area Legal.

In occasione di verifiche, ispezioni o accertamenti da parte di funzionari pubblici presso la sede della Società, il primo interlocutore dei funzionari è l'Amministratore Delegato che fornisce un'accoglienza istituzionale iniziale.

Successivamente, la gestione operativa delle attività di controllo è affidata al Responsabile della Funzione competente, supportato sempre da una seconda persona.

Le attività connesse alla gestione dei rapporti con le Autorità di Vigilanza sono svolte dai soggetti appositamente incaricati ai sensi del vigente sistema dei poteri e delle deleghe e in linea con la normativa interna, fatte salve diverse richieste da parte delle Autorità.

I Responsabili delle aree di volta in volta interessate provvedono a validare il contenuto dei flussi informativi e documentali verso le Autorità di Vigilanza, per quanto di propria competenza.

L'Amministratore Delegato è munito di poteri di firma per le comunicazioni aziendali verso le Autorità di Vigilanza, fatta salva la possibilità di conferire subdelega ad altri soggetti in relazione a determinate materie.

Ai sensi della politica di gestione dei rapporti con la Pubblica Amministrazione e Autorità di Vigilanza, anche in caso di ispezioni, la Società individua una figura di riferimento per la gestione, limitatamente agli accertamenti *on-site* dell'Autorità di Vigilanza (Consob, Banca d'Italia, CSSF), interfacciandosi con le aree di volte in volta interessate.

Il Consiglio di Amministrazione, il Collegio Sindacale, l'Amministratore Delegato, l'OdV e i Responsabili delle Funzioni Aziendali di Controllo sono sempre informati dell'eventuale avvio di ispezioni o richieste rilevanti delle Autorità di Vigilanza, nonché di eventuali prescrizioni o eccezioni rilevate dalle stesse.

Sono previsti momenti di coordinamento fra tutti i soggetti interessati e durante i quali avviene un confronto circa gli sviluppi dell'ispezione, le richieste ricevute e i punti di attenzione, al fine di valutare/ definire le attività da porre in essere.

Il contenuto di tutte le comunicazioni ricevute dalle Autorità e inviate alle stesse è verificato dai Responsabili delle aree di competenza, eventualmente con il supporto della funzione Compliance.

È manutenuto uno scadenziario dei principali flussi informativi dovuti alle Autorità di Vigilanza, predisposto in conformità alle normative di riferimento.

Relativamente a determinati flussi informativi verso le Autorità di Vigilanza, sono implementati controlli automatici attraverso i software diagnostici messi a disposizione dalle Autorità stesse.

Le aree competenti per la produzione di documenti e informazioni da trasmettere alle Autorità di Vigilanza provvedono alla relativa archiviazione presso la propria cartella di rete aziendale, unitamente alle eventuali evidenze allegate e/o a supporto.

I documenti richiesti dalle Autorità in sede ispettiva sono inviati dalle aree interessate a lla figura di riferimento per la gestione dell'ispezione, che provvede alla relativa archiviazione in un'area protetta della rete aziendale, appositamente messa a disposizione dell'Autorità.

I flussi informativi prodotti nell'ambito della gestione dei rapporti con Autorità di Vigilanza sono scambiati tramite posta elettronica (eventualmente certificata) e/o secondo altre modalità tali da garantirne la tracciabilità (ad esempio, canali telematici delle Autorità, ricevute di avvenuta trasmissione).

10.3. Tracciabilità delle operazioni

Devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate.

Non deve esservi identità soggettiva tra coloro che assumono e attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno.

L'articolazione funzionale o l'unità organizzativa, alla quale sia richiesta un'informazione dai soggetti competenti, deve fornire la documentazione idonea a rispondere al quesito formulato, attestando la provenienza e, ove possibile, la completezza e la veridicità delle informazioni, o indicando i soggetti che possono fornire tale attestazione.

10.3.1. Tracciabilità delle operazioni e sistema informatico

È prevista l'adozione di sistemi informatici, che garantiscano la corretta e veridica imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile, ai soggetti che vi partecipano ed al cliente, controparte o ente interessati.

Il sistema deve prevedere l'impossibilità di modifica delle registrazioni senza che ne risulti evidenza.

Ogni accesso alla rete informatica aziendale – sia intranet che internet – per l'effettuazione di operazioni ovvero per la documentazione di dette operazioni deve avvenire almeno con l'utilizzo di doppia chiave asimmetrica (user ID e password personale), o con altra procedura di non minore efficacia, che consenta all'operatore di collegarsi alla rete limitatamente alla fase della procedura di sua competenza e di lasciare evidenza non modificabile dell'intervento effettuato e dell'autore.

10.3.2. Archiviazione e conservazione documenti

I documenti riguardanti l'attività di Quaestio sono archiviati e conservati, a cura dell'area competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza.

Qualora il servizio di archiviazione o conservazione dei documenti sia svolto, per conto di Quaestio, da un soggetto ad essa estraneo, il servizio è regolato da un contratto nel quale si prevede, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a non permettere la modificazione successiva dei documenti, se non con apposita evidenza.

L'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a loro delegato, al Collegio Sindacale od organo equivalente o ad altri organi di controllo interno, alla società di revisione eventualmente nominata e all'Organismo.

10.4. Accesso e utilizzo del sistema informatico

L'accesso alle procedure informatiche è regolato attraverso definiti profili di utenza ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite a ciascun utente.

Sono previste modalità di utilizzo del sistema informatico basate su adeguato riscontro delle password di abilitazione per l'accesso ai sistemi informativi della P.A. eventualmente posseduti da determinati dipendenti appartenenti a specifiche funzioni o strutture aziendali.

Sono predisposti strumenti informatici che impediscano l'accesso e/o la ricezione del materiale relativo alla pornografia minorile e in generale limitino gli accessi a siti internet potenzialmente a rischio di reato.

È stabilito con chiarezza, e comunicato ai dipendenti e a tutti coloro che hanno accesso al sistema, l'ambito del corretto e consentito utilizzo, ovvero per fini aziendali, degli strumenti informatici in possesso dei dipendenti.

10.5. Trattamento dei dati personali

L'accesso ai dati personali in possesso di Quaestio ed il loro trattamento devono essere conformi al Regolamento UE 2016/679 (GDPR), anche come recepito in Italia, e successive modifiche e integrazioni, anche regolamentari.

L'accesso e il trattamento dei dati medesimi devono essere consentiti esclusivamente alle persone autorizzate e deve essere garantita la riservatezza nella trasmissione delle informazioni.

10.6. Sistema dei poteri e delle deleghe

Le procure devono essere coerenti con le deleghe interne.

Sono previsti meccanismi di pubblicità delle procure nei confronti degli interlocutori esterni.

Le deleghe sono attribuite secondo i principi di:

- autonomia decisionale e finanziaria del delegato;
- idoneità tecnico-professionale del delegato;
- disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Il soggetto munito di delega deve disporre di:

- poteri decisionali coerenti con le deleghe formalmente assegnate; un budget per l'efficace adempimento delle funzioni delegate, con la previsione di impegnare risorse eccedenti tale budget nel caso di eventi o situazioni di carattere eccezionale;
- di un obbligo di rendicontazione formalizzata, con modalità prestabilite, sulle funzioni delegate sufficienti a garantire un'attività di vigilanza senza interferenze;

10.7. Selezione di dipendenti, agenti, consulenti, collaboratori

La scelta dei dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle aree della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a questi criteri, la scelta deve essere motivata.

Il processo di selezione dei candidati deve prevedere almeno due colloqui conoscitivi:

- il primo svolto dai responsabili delle Aree interessate, rivolto alla selezione di una rosa di candidati;
- il secondo colloquio è svolto dal responsabile della Funzione HR e dall'Amministratore Delegato. Nel caso in cui il candidato venga assunto come dirigente, la proposta di assunzione deve essere portata in approvazione al Consiglio di Amministrazione.

Le assunzioni devono avvenire con regolare contratto di lavoro, nel rispetto di tutte le disposizioni normative vigenti nonché degli accordi contrattuali collettivi in essere, favorendo l'inserimento del lavoratore nell'ambiente di lavoro. In particolare, le funzioni competenti della Società devono verificare il possesso, da parte del soggetto con cui si intende avviare il rapporto di lavoro, di tutti i requisiti richiesti dalla legge per la permanenza e lo svolgimento dell'attività lavorativa richiesta nel territorio italiano. Analoghe verifiche devono essere esperite prima della conclusione di contratti di consulenza, agenzia, forme di lavoro parasubordinato, ovvero di appalto.

In sede di processo di assunzione il Responsabile dell'Area HR tiene adeguata traccia delle valutazioni effettuate sulla shortlist, sul candidato selezionato e sull'individuazione e gestione di eventuali conflitti di interesse. In questa fase, il Responsabile dell'Area HR richiede all'unità di Compliance di procedere alla consultazione del database di name screening a fini AML tempo per tempo adottato dalla SGR, con riferimento al nominativo del candidato selezionato.

Il Responsabile dell'Area HR richiede al candidato, il primo giorno di assunzione, di produrre un set di documenti necessari al perfezionamento del suo inserimento in azienda (a scopo esemplificativo e non esaustivo: codice fiscale, documenti di identità). Tra la documentazione necessaria per l'assunzione, il candidato dovrà altresì compilare la presa visione dell'informativa ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679.

Non è consentito:

- instaurare rapporti di lavoro, anche per contratti temporanei, senza il rispetto della normativa applicabile in materia (ex.: in termini di contributi previdenziali ed assistenziali, permessi di soggiorno), nonché delle disposizioni aziendali;
- inserire, nell'anagrafica del personale, dipendenti fittizi allo scopo di creare disponibilità extracontabili o per ottenere agevolazioni di qualsivoglia natura o esporre nella documentazione inviata o condivisa con enti pubblici fatti non rispondenti al vero, ovvero occultare fatti rilevanti;
- utilizzare metodi di sorveglianza dei lavoratori al di fuori di quanto previsto dalla normativa applicabile tempo per tempo in vigore;
- impiegare minori in attività lavorative al di fuori dei casi in cui ciò sia consentito dalla normativa applicabile tempo per tempo in vigore o per attività illecite;
- esporre i lavoratori a situazioni di pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

È fatto altresì espresso divieto di favorire, nei processi di assunzione, persone che siano state oggetto di segnalazione da parte di pubblici ufficiali, incaricati di pubblico servizio, dirigenti, funzionari, dipendenti o collaboratori di enti pubblici o privati, in cambio di favori, compensi o altri vantaggi per sé e/o per la Società. Non devono essere inoltre prese in esame eventuali segnalazioni provenienti da pubblici ufficiali, incaricati di pubblico servizio, dirigenti, funzionari, dipendenti o collaboratori di enti pubblici o privati ai fini dell'assunzione presso la Società di personale, o comunque dell'interessamento da parte della Società all'assunzione presso terzi. È in ogni caso fatto assoluto divieto di favorire, nei processi di assunzione di dipendenti o collaboratori, persone che siano state oggetto di segnalazione da parte di pubblici ufficiali, incaricati di pubblico servizio, dirigenti, funzionari, dipendenti o collaboratori di enti pubblici o privati, in cambio di favori, compensi o altri vantaggi per sé e/o per la Società.

10.8. Formazione del personale

Sono previste modalità efficienti per la formazione ed il costante aggiornamento dei dipendenti e dei collaboratori sulle regole e i presidi vigenti all'interno della struttura della Società posti a prevenzione dei reati di cui al Decreto.

10.8.1. Formazione del personale in materia di sicurezza e salute dei lavoratori

È diffuso tra i dipendenti un documento di politica interna, che stabilisce gli indirizzi e gli obiettivi generali del sistema di prevenzione e protezione volti a perseguire obiettivi di adeguata tutela in materia di salute e sicurezza.

È prevista la predisposizione di un calendario che prevede riunioni periodiche dei funzionari coinvolti per la verifica della situazione nella gestione delle tematiche afferenti alla salute e sicurezza.

È prevista una procedura che disciplini ruoli, responsabilità e modalità operative relativamente alla diffusione ai lavoratori delle informazioni periodiche e delle informazioni in caso di pericolo grave e immediato.

È prevista una disciplina relativa all'informativa al medico competente relativamente ai processi e rischi connessi all'attività produttiva.

10.9. Sistema di incentivazione e remunerazione

I sistemi premianti devono essere strutturati in modo pienamente conforme alla normativa applicabile alla Società e rispondere a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate.

Non devono essere previsti né corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, e a soggetti pubblicisticamente qualificati in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e con riferimento alle condizioni e alle prassi esistenti sul mercato nell'area geografica di riferimento o determinate da tariffe.

10.10. Selezione di fornitori, controparti commerciali e partners

La scelta dei fornitori di beni o servizi avviene, a cura della funzione competente, sulla base di requisiti di professionalità, affidabilità, economicità, pari trattamento, trasparenza nelle procedure di selezione.

Sono sempre definiti i requisiti minimi in possesso dei soggetti offerenti e la fissazione dei criteri di valutazione delle offerte prima della ricezione delle stesse.

Sono determinati specifici criteri di selezione, stipulazione ed esecuzione di accordi o joint venture con altre imprese per la realizzazione di investimenti, con particolare riferimento alla congruità economica degli investimenti effettuati in joint venture.

È prestata particolare attenzione nel valutare le possibili partnership commerciali con società operanti nei settori della comunicazione telematica (in relazione al rischio di diffusione di materiale pedopornografico) o di turismo in aree geografiche a rischio.

10.11. Regolamentazione dei rapporti con fornitori, consulenti, controparti contrattuali e partners

La SGR richiede ai soggetti esterni, ivi incluse le controparti commerciali, i consulenti e con i partners, anche attraverso apposite clausole l'impegno ad attenersi ai principi di cui al D.Lgs 231/01.

10.12. Gestione del processo di approvvigionamento beni e servizi

Non vi deve essere identità tra chi richiede la prestazione o chi la autorizza e chi esegue il pagamento della stessa. Devono essere chiaramente formalizzati i compiti, i poteri e le responsabilità attribuiti a ciascuno.

In assenza di specifica autorizzazione da parte della Funzione Compliance, ai fornitori o ai consulenti non è consentito cedere a terzi il diritto alla esecuzione della prestazione dedotta nel contratto o Il diritto alla riscossione del compenso, né è consentito loro attribuire a terzi il mandato all'incasso. Il relativo contratto deve contenere tali divieti, a meno che sia intervenuta la sopra prevista autorizzazione da parte della Funzione Compliance.

10.13. Gestione delle risorse finanziarie

Sono stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone.

Il processo inerente al pagamento dei fornitori deve essere formalizzato e improntato al principio di segregation of duties, in forza del quale il censimento del fornitore, la contabilizzazione della fattura ed il relativo pagamento devono essere svolte da soggetti distinti.

Le operazioni che comportano utilizzazione o impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità con i principi di professionalità e correttezza gestionale e contabile. Il processo decisionale deve essere verificabile.

L'impiego di risorse finanziarie deve essere motivato dal soggetto richiedente, che ne attesta la congruità.

In caso di operazioni ordinarie, se comprese entro la soglia quantitativa stabilita, la motivazione può essere limitata al riferimento alla classe o tipologia di spesa alla quale appartiene l'operazione.

Il superamento dei limiti di cui al punto precedente può avvenire solo nel rispetto delle vigenti procedure di autorizzazione e previa adeguata motivazione. Comunque, in caso di operazioni diverse dalle ordinarie o eccedenti la soglia quantitativa stabilita, la motivazione deve essere analitica.

Devono essere identificabili le provenienze formali e materiali del denaro e dei valori.

Tutte le operazioni di acquisizione, gestione e trasferimento di denaro o valori devono essere documentate, in ogni loro fase, a cura delle funzioni competenti, con la possibilità di individuare le persone fisiche intervenute nei passaggi.

Deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza dei destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione.

L'Area Amministrazione e Controllo deve per ogni acquisto verificare la coincidenza tra contratto/ordine di acquisto, fattura e documenti di trasporto nonché accertare, con la Funzione che ha emesso l'ordine/richiesto il contratto, l'effettiva consegna del bene o l'effettiva fornitura del servizio, contabilizzare l'operazione.

Il dipendente deve ottenere l'autorizzazione del responsabile del processo per il rimborso delle spese sostenute nell'ambito lavorativo.

Tutte le operazioni che comportano acquisizione, gestione e trasferimento di denaro o valori sono tracciate e riscontrabili, fermo comunque restando che:

(i) i pagamenti devono essere effettuati nel pieno rispetto della Normativa Applicabile e in primo luogo della normativa vigente in materia di strumenti di incasso e pagamento, tracciabilità dei flussi finanziari e antiriciclaggio, nonché delle disposizioni aziendali tempo per tempo vigenti;

(ii) non sono ammessi pagamenti su conti cifrati;

(iii) i pagamenti relativi ad obbligazioni della Società devono essere effettuati unicamente a favore dei soggetti nei confronti dei quali sussiste l'obbligo, salvo che sia intervenuta esplicita autorizzazione scritta da parte dell'Area Legal. Tale autorizzazione può essere concessa solo in presenza di giustificate motivazioni riportate nell'autorizzazione;

(iv) non possono essere effettuati pagamenti frazionati se non supportati da accordi scritti che espressamente li prevedono;

(v) fatto salvo quanto previsto nel precedente punto (iii), i pagamenti da effettuare mediante bonifico devono essere disposti esclusivamente su conti intestati ai fornitori stessi ed indicati da questi ultimi al momento della stipula del contratto o successivamente tramite comunicazione scritta;

(vi) vanno evitati pagamenti all'estero disposti a favore di soggetti residenti in Italia, salvo che ricorrano giustificate ragioni che devono risultare per iscritto. In tale ultimo caso è cura dell'Area Amministrazione e Controllo archiviare la documentazione dalla quale risulti la sussistenza delle ragioni giustificative alla base del pagamento all'estero;

(vii) i pagamenti sono disposti unicamente da soggetti muniti dei necessari poteri in base al sistema di deleghe e procure tempo per tempo vigente. Prima di procedere al pagamento, il soggetto legittimato ad effettuare il pagamento verifica che ricorrano tutte le condizioni, ivi comprese le autorizzazioni al pagamento, alla cui sussistenza le disposizioni aziendali subordinano l'effettuazione del pagamento stesso. Non si può procedere al pagamento laddove non risulti che sia stata effettuata, con esito positivo, tale verifica;

(viii) gli assegni bancari possono essere emessi, e l'emissione di assegni circolari può essere richiesta, soltanto da soggetti dotati di idonei poteri, anche di rappresentanza, sulla base del sistema di deleghe e procure tempo per tempo in vigore;

(ix) tutti i pagamenti e gli altri trasferimenti di valuta fatti dalla/alla Società anche dall'estero o all'estero, devono essere accuratamente ed integralmente registrati nei libri contabili e nelle scritture obbligatorie;

(x) non devono essere create registrazioni false, incomplete o ingannevoli, e non devono essere istituiti fondi segreti o non registrati, e neppure possono essere depositati fondi in conti personali o non appartenenti alla Società;

(xi) non deve essere fatto alcun uso non autorizzato di fondi della Società.

Devono essere effettuati periodici controlli formali e sostanziali dei flussi aziendali, con riferimento a pagamenti verso terzi e ai pagamenti delle operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte, degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e istituti che non hanno insediamenti fisici in alcun paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni ed operazioni straordinarie.

Spetta all'Area Amministrazione e Controllo, d'intesa con l'Area Legal:

a) individuare gli strumenti di pagamento diversi dai contanti che possono essere utilizzati dai soggetti interni per far fronte all'adempimento da parte della Società di obbligazioni ad essa facenti capo;

b) stabilire le modalità e le condizioni di utilizzo e di impiego degli strumenti di pagamento diversi dai contanti individuati ai sensi del punto a) che precede, tenuto conto della normativa applicabile e delle disposizioni aziendali tempo per tempo vigenti.

10.14. Rapporti economico-finanziari con la P.A. o i suoi esponenti

I contatti con esponenti della P.A. devono essere specificamente motivati.

Deve essere previsto un obbligo di immediata informativa all'Organismo in caso di proposte o richieste illecite o sospette avanzate da appartenenti alla P.A. o da soggetti pubblicisticamente qualificati.

10.15. Rapporti con intermediari finanziari

La Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie e ai fini dell'attuazione delle operazioni di acquisizione, gestione o trasferimento di denaro o valori, deve avvalersi di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea.

È obbligatorio utilizzare esclusivamente, nell'ambito della gestione delle transazioni finanziarie, operatori finanziari muniti di presidi manuali e informatici idonei a prevenire fenomeni di riciclaggio nazionale o internazionale.

È fatto divideto di:

- utilizzare contante per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie in violazione della normativa applicabile e delle disposizioni aziendali tempo per tempo vigenti. Tutti i pagamenti per cassa, nonché i prelevamenti e gli eventuali incassi devono essere registrati in apposito registro, tenuto dall'Area Amministrazione e Controllo. I prelevamenti per cassa devono essere autorizzati dal Responsabile dell'Area Amministrazione e Controllo, il quale provvede anche a effettuare mensilmente una riconciliazione tra registrazioni riportate nel registro e consistenze del fondo. Non possono essere in alcun caso effettuati prelevamenti per importi giornalieri superiori a euro 350,00 o per importi cumulativi settimanali superiori a euro 1.500,00. Il fondo cassa non può superare in nessun momento l'importo di euro 1.500,00 o il minore importo previsto dalla Normativa Applicabile di tempo in tempo vigente;

- accettare ed eseguire ordini di pagamento provenienti da soggetti non identificabili.

10.16. Antiriciclaggio e antiterrorismo

Il Consiglio di Amministrazione nomina il Responsabile dei controlli, che è anche Responsabile Antiriciclaggio - cui spetta anche il ruolo di Responsabile per le segnalazioni aggregate antiriciclaggio alle autorità di vigilanza e il ruolo di Delegato per la segnalazione delle operazioni sospette.

La società predispone specifici piani formativi interni - approvati dal Consiglio di Amministrazione - per il personale in tema di contrasto al riciclaggio e al finanziamento del terrorismo.

I destinatari devono informare immediatamente il proprio superiore gerarchico rispetto all'eventuale sussistenza di conflitti d'interesse nello svolgimento di attività valutative/autorizzative inerenti all'attività antiriciclaggio e antiterrorismo, astenendosi peraltro dall'attività per rimetterla ad altri soggetti competenti e autorizzati.

I destinatari sono tenuti a sospendere immediatamente l'attività qualora non sia chiara la provenienza del denaro/beni/altra utilità oggetto di operazione oppure quando vi siano elementi tali da far sospettare una provenienza delittuosa.

È previsto l'obbligo di approfondire e aggiornare la conoscenza della controparte al fine di valutare la coerenza e la compatibilità dell'operazione richiesta con il suo profilo economico finanziario.

È sempre verificata l'attendibilità e affidabilità commerciale e professionale dei clienti sulla base di alcuni indici rilevanti quali: procedure concorsuali, acquisizione di informazioni commerciali sull'azienda, sui soci e sugli amministratori tramite società specializzate, coinvolgimento di persone politicamente esposte.

È prevista la rilevazione e l'immediata segnalazione di operazioni ritenute anomale o sospette per controparte, tipologia, oggetto, frequenza o entità.

In caso di profili di anomalia di qualunque natura nei rapporti finanziari con il fornitore o con il cliente, il rapporto è mantenuto sulla base di espressa autorizzazione dell'Amministratore Delegato.

È previsto l'obbligo di evidenziare ed immediatamente segnalare le operazioni poste in essere da un soggetto in nome, per conto o a favore di terzi in assenza di legami familiari o relazioni commerciali idonee a giustificarle ovvero le operazioni poste in essere da soggetti terzi in favore delle controparti, in assenza di ragioni giustificatrici.

Gli elementi da considerare nella valutazione di una operazione sospetta sono:

- importo operazione;
- modalità esecuzione;
- destinatario operazione;
- localizzazione territoriale.

Il personale a diretto contatto con la clientela deve segnalare la circostanza al Responsabile di Funzione.

10.17. Trasferimenti di beni aziendali

Per le operazioni di acquisizione e dismissione di società o rami d'azienda, è preventivamente verificata la provenienza dei beni conferiti nel patrimonio della società o del ramo di azienda da acquistare nonché l'identità, la sede, la natura giuridica, la certificazione antimafia del soggetto cedente.

10.18. Rilevazione, registrazione e rappresentazione dell'attività societaria nelle scritture contabili, nei bilanci, nelle relazioni ed in altri documenti

In ogni articolazione funzionale o unità organizzativa competente sono adottate misure idonee a garantire che le operazioni contabili siano effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza e siano tempestivamente segnalate eventuali situazioni anomale.

Sono previste misure idonee a garantire che l'informazione comunicata ai soggetti gerarchicamente sovraordinati da parte dei responsabili dell'articolazione funzionale o dell'unità organizzativa competente sottordinata sia veritiera, corretta, accurata, tempestiva e documentata, anche con modalità informatiche.

È previsto l'obbligo per il responsabile di funzione che fornisce dati ed informazioni relativi al bilancio o ad altre comunicazioni sociali di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse con affermazioni precise, analitiche e documentabili.

Sono previste misure idonee ad assicurare che, qualora siano formulate richieste, da chiunque provenienti, di atipica variazione quantitativa dei dati, rispetto a quelli già contabilizzati in base alle procedure correnti, chi ne sia a conoscenza informi, senza indugio, l'Organismo.

Sono previste misure idonee a garantire che, qualora siano formulate ingiustificate richieste di variazione dei *criteri* di rilevazione, registrazione e rappresentazione contabile, chi ne sia a conoscenza informi, senza indugio, l'Organismo.

Deve essere previsto l'obbligo per chi fornisce informazioni previste alle unità gerarchicamente sovraordinate di indicare i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, al fine di garantire la verificabilità delle stesse. Le copie dei documenti richiamati devono essere rese disponibili.

In merito alla gestione di acquisti di beni e servizi è prevista la firma del contratto da parte del personale autorizzato e una costante verifica della corrispondenza dell'importo con quanto pattuito contrattualmente.

Con riferimento alla gestione delle note spese da parte del personale esiste un controllo periodico dei rimborsi spese e del loro corretto riporto nei cedolini. I rimborsi spese da parte dei soggetti titolati inoltre avviene solo previa autorizzazione e previa verifica dei presupposti (inerenza, presenza dell'autorizzazione alla trasferta, etc).

Devono essere adottate misure idonee ad assicurare che i dipendenti, i collaboratori e i consulenti tenuti al rispetto delle previsioni del presente Modello, nell'àmbito delle rispettive competenze:

(i) non emettano fatture o rilascino altri documenti aventi rilevanza fiscale per operazioni inesistenti o solo in parte esistenti comunque volte a consentire, anche a soggetti terzi, di commettere un'evasione fiscale o di ottenere benefici o vantaggi non dovuti;

(ii) non siano oggetto di registrazione o, comunque, non siano utilizzati fatture o altri documenti aventi rilevanza fiscale per operazioni inesistenti o solo in parte esistenti;

(iii) siano previsti ed effettivamente attuati controlli volti ad assicurare il rispetto delle previsioni dei precedenti punti (i) e (ii);

(iv) le scritture contabili e gli altri documenti (tra cui i documenti di trasporto) di cui sia obbligatoria la conservazione ai fini fiscali, siano archiviati in modo corretto ed ordinato, anche approntando difese fisiche e/o informatiche che impediscano atti di distruzione, di occultamento o di modifica non autorizzata.

Nella predisposizione delle dichiarazioni relative alle imposte sui redditi e sul valore aggiunto è fatto in oigni caso divieto ai dipendenti, ai collaboratori e ai consulenti, nell'àmbito delle rispettive competenze, di:

- indicare elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti;
- indicare elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi (ex.: costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
- indicare una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi;
- far inutilmente decorrere i termini, previsti dalla normativa applicabile, per la presentazione delle dichiarazioni medesime o per il successivo versamento delle imposte da esse risultanti.

Il Responsabile dell'Area Amministrazione e Controllo è tenuto ad assicurare, anche attraverso specifiche procedure, l'attuazione del principio di segregazione dei ruoli in relazione all'attività di gestione della contabilità aziendale e nella successiva trasposizione nei bilanci e nelle dichiarazioni fiscali con riferimento alle seguenti attività:

- controllo sull'effettività delle prestazioni rispetto alle fatture o agli altri documenti fiscali emessi;
- verifica della veridicità dei bilanci e delle dichiarazioni fiscali rispetto alle scritture contabili;
- verifica della corrispondenza tra gli importi delle imposte liquidate e importi effettivamente versati;
- verifica della corrispondenza tra i certificati rilasciati in qualità di sostituto di imposta e l'effettivo versamento delle relative ritenute.

10.19. Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato e alla stipulazione di contratti derivati non negoziati su mercati regolamentati italiani ed europei

Per la compravendita di strumenti finanziari da parte della SGR il Consiglio di Amministrazione ha adottato una delibera quadro alla quale deve uniformarsi l'operatività.

Sono stati introdotti principi, regolamenti e procedure in tema di abusi di mercato anche mediante riferimento alla casistica riportata dalla Consob e dalle altre autorità di vigilanza o controllo, anche in sede consultiva.

Sono state formalizzate procedure per l'effettuazione di operazioni in partecipazioni rilevanti su strumenti finanziari non quotati. L'effettuazione delle operazioni deve essere condizionata all'autorizzazione da parte del Consiglio di Amministrazione su proposta del Comitato Investimenti.

È prevista l'individuazione delle controparti con le quali tali operazioni possono essere di norma effettuate e dei limiti fissati per la gestione degli investimenti e dei rischi collegati.

È previsto che le procedure contengano la definizione dei soggetti competenti a decidere le operazioni, ad attuarle e ad effettuare attività di controllo e vigilanza sulle stesse.

Sono determinati i relativi livelli quantitativi di autorizzazione e approvazione.

Qualora la controparte negoziale non sia un intermediario finanziario sottoposto a vigilanza prudenziale, di correttezza e di trasparenza conformi alla legislazione dell'Unione Europea, la funzione competente all'assunzione della decisione deve fornire una documentata motivazione dell'operazione e del prezzo stabilito per la stessa.

I contratti derivati sono stipulati secondo modelli contrattuali riconosciuti dalla migliore prassi internazionale (Isda).

10.20. Comunicazione di informazioni relative ad operazioni significative della Società o di società in cui Quaestio Holding S.A. detenga una partecipazione ed aventi ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazioni in un mercato regolamentato

Sono previste misure idonee a garantire la veridicità, la completezza e la correttezza delle informazioni concernenti la Società destinate al mercato.

Sono previste misure idonee a garantire che le informazioni rilevanti comunicate internamente mediante posta elettronica siano protette da eventuali rischi di diffusione impropria.

10.21. Operatività in strumenti finanziari quotati

È definita e formalizzata una *policy* riguardante la gestione degli investimenti finanziari e dei rischi collegati, l'identificazione degli strumenti finanziari che possono essere oggetto di operazioni da parte della Società, dei relativi livelli quantitativi di autorizzazione ed approvazione, delle controparti con le quali tali operazioni possono essere di norma effettuate e dei limiti fissati per la gestione degli investimenti e dei rischi collegati.

Sono definiti e descritti principi e regole operative concernenti il compimento di operazioni sugli strumenti finanziari, differenziando, qualora necessario, le regole in funzione della tipologia di strumento finanziario e della motivazione

dell'operazione. Tali procedure devono contenere la definizione dei soggetti competenti a decidere le operazioni, ad attuarle e ad esercitare attività di controllo e vigilanza sulle stesse.

Sono definite regole, modalità e procedure, anche informatiche, volti a garantire la separazione - sul piano soggettivo - tra coloro che hanno il potere di rappresentanza - anche con facoltà di delega - in merito ad operazioni bancarie e coloro che hanno potere di rappresentanza in merito al compimento di operazioni aventi ad oggetto gli strumenti finanziari.

10.22. Gestione delle informazioni privilegiate

Sono in generale adottate specifiche procedure per la formazione, l'attuazione, la comunicazione interna ed esterna delle decisioni della Società e degli eventi che accadono nella sfera di attività della stessa.

Sono identificate le aree di attività della Società dove di norma si formano, vengono aggiornate, comunicate e gestite le informazioni privilegiate.

Sono identificate, all'interno della Società, le informazioni privilegiate o destinate a diventare privilegiate (anche mediante la predisposizione di elenchi esemplificativi), nonché i criteri idonei a qualificare le informazioni come privilegiate o destinate a divenire tali. In particolare, qualora l'informazione riguardi eventi o procedimenti decisionali a più fasi, la definizione di informazione privilegiata dovrà indicare i criteri per valutare il momento a partire dal quale l'informazione stessa debba essere sottoposta alle procedure di gestione delle informazioni privilegiate (informazione destinata a diventare privilegiata); nella definizione in oggetto dovranno essere considerate le comunicazioni, istruzioni e raccomandazioni delle Autorità di Vigilanza e controllo, anche in riferimento agli elenchi di operazioni sospette elaborati da organi dell'Unione Europea (come l'ESMA). La precisazione dei criteri di identificazione delle informazioni privilegiate o destinate a divenire tali, deve essere effettuata a cura della funzione compliance e sottoposta al parere dell'Organismo.

È prevista - se del caso - una procedura per l'individuazione del momento in cui l'informazione privilegiata o destinata a divenire tale deve essere oggetto di comunicazione al pubblico e per l'identificazione del soggetto competente alla comunicazione.

È assicurata la riservatezza delle informazioni privilegiate o destinate a diventare privilegiate, all'interno della Società, sia nel caso in cui l'informazione si trovi su supporto informatico sia che si trovi su supporto cartaceo.

Sono assicurate misure idonee a prevenire ed evitare la comunicazione impropria e non autorizzata all'interno o all'esterno della Società delle informazioni privilegiate o destinate a diventare privilegiate.

Sono assicurate misure idonee a garantire specificamente che le informazioni rilevanti comunicate internamente mediante posta elettronica siano protette da eventuali rischi di diffusione impropria.

Sono inoltre adottate misure per proteggere, conservare e aggiornare le informazioni che, laddove queste riguardino procedimenti a più fasi, integrano il contenuto delle informazioni stesse.

La necessità che i documenti contenenti informazioni privilegiati siano classificati come "confidenziali"/riservati, presentino nomi in codice per salvaguardare la natura riservata dell'informazione, siano protetti da password e custoditi in locali ad accesso fisico controllato o in archivi custoditi nonché eliminati con le modalità che ne rendano impossibile il recupero del contenuto informativo.

Sono in generale assicurate misure idonee ad evitare la comunicazione selettiva di informazioni privilegiate e destinate a divenire privilegiate.

Sono identificate le persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, gestiscono le informazioni privilegiate o destinate a divenire privilegiate; i nominativi delle persone predette sono inseriti in un registro informatico, con idonei presidi per garantirne la conservazione e la non modificabilità, se non con apposita evidenza; l'inserimento nel registro deve essere comunicato al soggetto interessato al fine di imporre l'osservanza delle procedure e dei divieti conseguenti; parimenti deve avvenire per le persone che hanno accesso alle informazioni privilegiate o destinate a divenire privilegiate; è inoltre identificato un responsabile dei registri contenenti i nominativi delle persone di cui sopra, ai fini della vigilanza sul suo corretto funzionamento, del controllo relativo alla tutela della riservatezza e dell'aggiornamento, con accesso al registro stesso e alle informazioni ivi contenute.

È impedito l'accesso, anche accidentale, a informazioni privilegiate da parte di persone diverse da quelle regolarmente autorizzate, nonché la circolazione, anche interna alla Società, delle informazioni stesse in modo improprio. In particolare i documenti contenenti informazioni privilegiate o destinate a diventare tali, devono essere archiviati e conservati, a cura della funzione competente e del responsabile incaricato - in luoghi - anche informatici - ad accesso limitato e adeguatamente presidiati. In particolare, l'archiviazione deve avvenire con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza dell'accesso ai documenti già archiviati; l'accesso a questi ultimi è sempre motivato e consentito solo alle persone autorizzate in base alle norme interne. Copie dei documenti contenenti informazioni privilegiate devono essere consegnate solo alle persone autorizzate ed eventuali copie in eccesso devono essere distrutte al termine di eventuali riunioni.

In caso di legittima comunicazione dell'informazione privilegiata a soggetti esterni alla Società (ad esempio consulenti, società di revisione), devono essere predisposte clausole contrattuali che vincolino la parte terza alla riservatezza dell'informazione, eventualmente prevedendo l'adozione, da parte di tali soggetti, di idonee misure di protezione dell'informazione ricevuta.

I rapporti con investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o con il pubblico in generale sono tenuti esclusivamente da soggetti appartenenti alle funzioni competenti (almeno due, tra cui il responsabile della funzione), nel rispetto dei tempi e delle modalità stabilite dalla legge, dalle Autorità di Vigilanza del mercato e dalle procedure contemplate dal sistema di controllo interno.

L'organizzazione e la partecipazione agli eventuali incontri, in qualunque forma tenuti, con investitori, analisti finanziari, giornalisti o altri rappresentanti dei mezzi di comunicazione di massa, devono avvenire esclusivamente a cura delle funzioni competenti e nel rispetto delle vigenti procedure di autorizzazione e di controllo interno.

Sono stabilite misure idonee per verificare e controllare in via preventiva la legittimazione alla partecipazione e i contenuti da trattare negli incontri, in qualunque forma tenuti, con investitori, giornalisti o altri rappresentanti dei mezzi di comunicazione di massa.

A salvaguardia della veridicità e completezza delle informazioni, sono stabilite misure idonee a verificare i contenuti dei prospetti, dei documenti informativi, dei comunicati, del materiale informativo in qualunque forma predisposto, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa, al mercato od al pubblico in generale.

10.23. Gestione del sistema di prevenzione e protezione della sicurezza e salute dei lavoratori

E' prevista la nomina di un RSPP che monitora il rispetto degli obblighi in tema di salute e sicurezza dei lavoratori, tra cui:

- la trascrizione e l'archiviazione dei risultati degli accertamenti sanitari dei singoli lavoratori nelle Cartelle Sanitarie e di Rischio;
- le modalità operative per la nomina dei lavoratori incaricati dell'attuazione delle misure di prevenzione, di emergenza e di primo soccorso;le modalità operative per la gestione della segnaletica di sicurezza;
- la redazione del documento di valutazione dei rischi in relazione a i) rischi specifici professionali, ii) rischi per lavoratrici gestanti, iii) rischi stress lavoro correlati;
- le modalità operative per l'accesso dei lavoratori in aree a rischio per la salute e sicurezza;
- le modalità operative, i ruoli e le responsabilità in caso di eventuali situazioni di emergenza;
- le modalità operative per l'abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato;
- le misure organizzative per l'individuazione dei tempi e delle modalità per l'effettuazione della richiesta del rilascio o rinnovo della scia incendio (ex CPI DPR 151/2011), nonché del rilascio del nullaosta provvisorio.

È definito e collaudato (anche mediante prove di emergenza) un piano di emergenza ed una procedura di gestione delle emergenze atta a mitigare gli effetti sulla salute della popolazione e sull'ambiente esterno.

È previsto un dovere di valutazione del rischio di incendio, di predisposizione ed aggiornamento del registro antincendio, di predisposizione di un piano di emergenza.

10.24. Gestione degli strumenti informatici

È 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 soggetti 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, troian, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative a 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 a 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 condotte tali da costituire violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:
- diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;
- abusivamente duplicare, detenere o diffondere in qualsiasi forma programmi per elaboratore od opere audiovisive o letterarie;
- detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;

In relazione alla tutela della riservatezza ed accesso ai dati*:*

- le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione e conservazione, in modo tale da risultare accessibili esclusivamente a coloro i quali sono autorizzati a conoscerle, e, in generale, ogni specifico dato deve essere utilizzato esclusivamente da soggetti autorizzati (c.d. principio di riservatezza);
- deve essere predisposto un sistema di protezione idoneo ad identificare ed autenticare univocamente gli utenti che intendono ottenere l'accesso ad un sistema elaborativo o trasmissivo;
- deve essere realizzato un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichi attraverso la gestione e la verifica dei diritti d'accesso;
- l'autenticazione deve essere effettuata prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.

In relazione all'integrità dei dati:

- deve essere assicurato che ogni dato aziendale corrisponda a quello originariamente immesso nel sistema informatico o che risulti modificato in modo legittimo e che le informazioni non possano essere manomesse o modificate da soggetti non autorizzati (c.d. principio di integrità).

In relazione alla disponibilità dei dati:

- i dati aziendali devono essere sempre reperibili in conformità alle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica (c.d. principio di disponibilità).

In relazione al non ripudio:

- devono essere applicate misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute (c.d. non ripudio).

In relazione alla sicurezza informatica ed alle verifiche della vulnerabilità:

- devono essere esaustivamente identificate e classificate le risorse e le relative vulnerabilità ovvero le carenze di protezione con riferimento ad una determinata minaccia ed alle seguenti componenti: a) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti); b) hardware; c) software; d) documentazione; e) dati e informazioni; f) risorse umane;
- devono essere compiutamente individuate le minacce, interne ed esterne, cui possono essere esposte le risorse;
- in generale, deve essere puntualmente pianificata e periodicamente aggiornata una attività di sicurezza informatica con previsione di un sistema di protezione preventivo;

- deve essere predisposta ed attuata una policy aziendale che stabilisca le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi ed un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole;
- devono essere preventivati i potenziali danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della probabilità di accadimento e delle possibili contromisure in base ad un'analisi costi-benefici degli investimenti per la predisposizione delle stesse;
- deve essere definito un ampio piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
- deve essere documentato ed espressamente accettato il rischio residuo.

In relazione alla sicurezza informatica ed alla continuità nei servizi informatici:

- deve essere definito un sistema di emergenza, ovvero devono essere predisposte tutte le procedure tecnico-organizzative per poter affrontare stati di emergenza e garantire la continuità delle operazioni attraverso meccanismi di superamento di situazioni anomale;
- sono previsti ed attuati processi e meccanismi che garantiscano la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti di protezione del trasferimento dati, al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi ed alle componenti di networking.

In relazione alla sicurezza informatica ed alle analisi degli eventi informatici:

- deve essere effettuata una compiuta attività di analisi degli eventi registrati volta a rilevare ed a segnalare eventi anomali che, discostandosi dagli standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.

In relazione alla sicurezza informatica ed alla registrazione degli eventi informatici:

- deve essere predisposto un sistema di tracciamento e monitoraggio degli eventi ed interventi di messa in sicurezza della rete.

In relazione alla predisposizione di copie di sicurezza:

- deve essere previsto il salvataggio di copia di backup dei dati a frequenze prestabilite.

In relazione alla verifica della qualità dei dati:

- devono essere istituiti presidi di carattere tecnologico volti alla verifica preventiva ed al monitoraggio continuo sulla qualità dei dati e la performance dei prodotti HW-SW.

In relazione alla sicurezza fisica, in particolare della sala server:

- deve essere assicurata la sicurezza fisica dei siti ove risiedono i sistemi di IT;

- deve essere organizzato un sistema di gestione delle credenziali fisiche.

In relazione alle procedure interne relative alle istruzioni operative ed alla gestione degli account:

- deve essere regolamentata la creazione, la modifica e la cancellazione di account e profili;
- è prevista una password o codici di valutazione per l'accesso ad ogni terminale che devono essere conosciute esclusivamente dal personale preposto;
- devono essere predisposte procedure formali per l'assegnazione di privilegi speciali (ad es. amministratori di sistema, super user).

In relazione alla definizione di un inventario logico-fisico relativo all'hardware e software:

- deve essere predisposto un inventario dell'hardware e del software in uso agli utenti che deve essere costantemente aggiornato;

In relazione alla sicurezza informatica, con particolare riferimento ai log ed ai relativi accessi:

- deve essere effettuata una review periodica dei log dagli amministratori di sistema in ambiente di produzione;
- deve essere impedito agli operatori di sistema accedere a sistemi o dati diversi da quelli sui quali sono stati chiamati a operare;
- deve essere effettuato costantemente il tracciamento degli accessi degli utenti alla rete aziendale;

In relazione alla sicurezza informatica, con particolare riferimento agli accessi agli ambienti di produzione:

- deve essere realizzata una corretta separazione tra gli ambienti di sviluppo, test e produzione.

In relazione alla sicurezza informatica, con particolare riferimento alla crittografia:

- è applicata una politica per l'uso di controlli crittografici per la protezione delle informazioni;
- è regolamentato il processo di generazione, distribuzione ed archiviazione delle chiavi.

In relazione al riutilizzo dei supporti di memorizzazione:

- sono previsti strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).

In relazione alle tematiche relative al trattamento dei dati personali:

- sono adottate misure minime di sicurezza per il trattamento di dati personali effettuati con strumenti elettronici (sistemi di autenticazione, di autorizzazione, antivirus, backup);

In relazione alla definizione di procedure e istruzioni operative relative alla sicurezza per il personale interno:

- devono essere definite politiche di sicurezza delle informazioni – gestione ed uso delle password, modalità di effettuazione dei log-in e log-out, uso della posta elettronica, modalità di utilizzo dei supporti rimovibili, l'uso dei sistemi di protezione (antivirus, antispam, antiphishing, antispy).

In relazione alla sensibilizzazione e formazione del personale interno:

- è attuata una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali;
- sono redatti, diffusi e conservati documenti normativi, tecnici, di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.

In relazione alla gestione dei rapporti con i fornitori di servizi/prodotti informatici:

- sono periodicamente verificati i rapporti con i fornitori di servizi informatici e siano introdotte, nei relativi contratti, adeguate clausole di tutela;
- sono predisposti con periodicità IT assessment in particolare quando si tratti di servizi gestiti in outsourcing.

In relazione alla gestione degli incidenti:

- devono essere tempestivamente segnalati alle competenti aree eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) con messa a disposizione ed archiviazione di tutta la documentazione relativa all'incidente e con attivazione di eventuale iter che può condurre all'eventuale apertura di uno stato di crisi;
- le risorse e i dispositivi informatici assegnati (personal computer, telefoni cellulari, etc.) devono essere utilizzati nel rispetto di principi di correttezza e diligenza ed esclusivamente ai fini dell'espletamento delle attività per cui sono stati assegnati. Devono inoltre tempestivamente informare le competenti aree della SGR in caso di eventuali furti o danneggiamenti.

10.25. Operazioni con parti correlate

Le operazioni con parti correlate devono essere effettuate in conformità alla normativa applicabile ed alle disposizioni aziendali, fermo in ogni caso restando che:

(i) è presente e aggiornato un elenco dei soggetti (persone fisiche e persone giuridiche) che possono essere qualificati come parti correlate della Società;

(ii) le operazioni con parti correlate devono essere effettuate nel rispetto della normativa applicabile e dei principi base dell'utilità, dell'inerenza e del confronto;

(iii) i rapporti con parti correlate devono essere definiti mediante accordi o ordini scritti sottoscritti o impartiti da soggetti che abbiano i relativi poteri di rappresentanza sulla base del sistema dei poteri in vigore e devono essere tracciabili;

(iv) la determinazione dei prezzi di trasferimento di beni e/o servizi deve avvenire sulla base del principio di libera concorrenza e comunque in modo conforme con la normativa tributaria applicabile alla Società in tema di transfer pricing tempo per tempo vigente;

(v) prima che il contratto sia sottoscritto e con il supporto delle altre Funzioni interessate, la Funzione Amministrazione verifica la determinazione dei prezzi pattuiti siano conformi alle previsioni delle Disposizioni Aziendali;

(vi) nel caso di contratti a prestazioni corrispettive, successivamente alla sottoscrizione del contratto, la Funzione Amministrazione verifica che la Società abbia effettivamente e regolarmente ricevuto le prestazioni cui aveva diritto, anche al fine di garantire una corretta registrazione nel periodo contabile di riferimento.

La documentazione a supporto delle operazioni, inclusa quella prevista dalla normativa tributaria, deve essere idonea a dimostrare le verifiche effettuate per dare attuazione alle disposizioni sopra riportate e va conservata ed archiviata a cura della Funzione Amministrazione in conformità alle Disposizioni Aziendali.

11. PRESIDI ORGANIZZATIVI ESISTENTI

La Società, per ciascuna area che presenta profili di rischio ai sensi del Decreto, dispone di articolati e strutturati presidi organizzativi.

11.1. Funzione Internal Audit

In riferimento alla funzione Internal Audit, sono state individuate le seguenti attività sensibili:

- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- gestione dei rapporti con il Collegio Sindacale;
- gestione dei rapporti con la Società di revisione;
- accesso al sistema informatico o database di terzi;
- archiviazione della documentazione;
- gestione del processo di selezione dei fornitori e di *outsourcer*;
- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.1.1. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

La gestione dei rapporti con le Autorità di Vigilanza prevede il coinvolgimento di diversi Organi e soggetti, anche appartenenti a Aree differenti.

In generale, secondo quanto previsto dal sistema dei poteri e delle deleghe della SGR l'Amministratore Delegato e il Presidente hanno il potere di rappresentare la Società davanti a uffici pubblici e di firmare la corrispondenza.

Con specifico riferimento ai flussi informativi da/verso le Autorità di Vigilanza che vedano coinvolta la funzione Internal Audit (es. Relazione annuale della funzione):

- la funzione Internal Audit produce e fornisce i contenuti di propria competenza;
- possono essere previsti momenti di condivisione/approvazione con altre aree/ organi/ funzioni/ unità. In particolare, la Relazione Annuale della funzione è portata in approvazione al Consiglio di Amministrazione e i flussi informativi la cui produzione preveda il coinvolgimento di più aree sono verificati in termini di coerenza e correttezza e completezza in fase di consolidamento delle informazioni da parte del soggetto volta per volta competente;

- le competenti aree della SGR provvedono alla trasmissione del flusso all'Autorità, mantenendone evidenza.

In riferimento a eventuali ispezioni/richieste da parte delle Autorità di Vigilanza, fatte salve diverse e specifiche disposizioni delle Autorità medesime, sono per prassi in essere le seguenti modalità di gestione:

- per le materia di propria competenza, la funzione Internal Audit partecipa a momenti di coordinamento e/o allineamento;
- la funzione Internal Audit produce le informazioni ed i documenti da fornire, richiesti dalle Autorità, nel rispetto delle previsioni normative applicabili nella materia rilevante;
- i documenti e le informazioni richiesti sono quindi inviati alla funzione Compliance, che provvede ad archiviarli in un'area protetta della rete aziendale, appositamente messa a disposizione dell'Autorità.

La funzione Internal Audit archivia presso la propria cartella di rete aziendale i documenti e le informazioni prodotte e trasmesse.

I flussi informativi verso le Autorità e le comunicazioni intercorrenti con i funzionari, nonché eventuali connesse comunicazioni interne e/o con gli outsourcer, sono generalmente effettuate tramite posta elettronica/ PEC e, comunque, mediante modalità che ne garantiscono la tracciabilità.

Il Codice Etico e di Comportamento adottato dalla SGR specifica che qualsiasi relazione con le Istituzioni deve svolgersi in maniera trasparente, rigorosa e coerente, nel rispetto della normativa vigente e sulla base di principi di correttezza e lealtà, evitando comportamenti volti a influenzare impropriamente ed indebitamente le attività e le decisioni delle Istituzioni.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Politica di gestione dei rapporti con la Pubblica Amministrazione e Autorità di Vigilanza, anche in caso di ispezioni.

11.1.2. Gestione dei rapporti con il Collegio Sindacale

Il Collegio Sindacale effettua le attività di controllo di propria competenza principalmente attraverso:

- apposite interviste ai referenti delle aree che presidiano l'ambito oggetto della specifica verifica;

- la partecipazione a momenti di coordinamento e di confronto che vedono riunite le Funzioni Aziendali di Controllo, le aree aziendali di volta in volta interessate e gli altri Organi societari. In particolare, i Sindaci partecipano ad ogni adunanza del Consiglio d'Amministrazione, avendo accesso ai relativi verbali nonché a tutto il materiale relativo agli argomenti all'ordine del giorno.

Con riferimento alle attività di controllo, sono previsti incontri di norma trimestrali con le Funzioni Aziendali di Controllo e le Aree della SGR di volta in volta interessate in relazione ai quali è prevista una preventiva convocazione da parte del Collegio Sindacale (tramite e-mail) ed eventualmente la produzione di documentazione da presentare nell'incontro pianificato, a supporto delle attività di verifica. In sede di incontro, i Sindaci approfondiscono le tematiche con i referenti intervistati.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura di revisione interna;
- Regolamento del Consiglio di Amministrazione e dei Comitati endo-consiliari.

11.1.3. Gestione dei rapporti con la Società di revisione

L'Assemblea della Società, su proposta del Consiglio di Amministrazione, ha affidato l'incarico di revisione legale, mediante apposito mandato, ad una società iscritta in apposito Albo.

L'Area Controlli partecipa a incontri dedicati, su richiesta della Società di revisione, in cui possono illustrare gli esiti delle proprie verifiche o portare elementi rilevanti in merito al funzionamento del sistema dei controlli interni.

L'Area Amministrazione e Controllo coordina l'attività di raccolta e la produzione della documentazione richiesta dalla Società di revisione, assegnando le connesse attività ai soggetti competenti della SGR e/o agli outsourcer. La stessa valida le informazioni eventualmente prodotte a fronte di specifiche richieste prima di autorizzarne il rilascio alla Società di revisione.

All'esito del processo di verifica posto in essere, la Società di revisione rilascia apposito giudizio, sotto forma di relazione, che viene sottoposta all'Assemblea.

I flussi informativi e documentali da/verso la Società di revisione, nonché trasmessi internamente funzionalmente all'evasione delle richieste della Società stessa, avvengono tramite e-mail. I documenti a supporto dei flussi informativi sono archiviati dalle Strutture competenti per materia.

Il responsabile dell'area Amministrazione e Controllo è sempre informato in merito agli sviluppi relativi ai rapporti con la società di revisione ed è messo in copia conoscenza nelle e-mail. Nelle comunicazioni ufficiali è messo in c/c anche l'Amministratore Delegato.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario.

11.1.4. Accesso al sistema informatico o database di terzi

L'accesso al sistema informatico o a database di terze parti deve avvenire esclusivamente in base a concessione delle terze parti, per le sole finalità connesse alla missione dell'unità organizzativa.

I software e gli applicativi che vengono utilizzati, anche per dialogare con applicativi e sistemi informatici di terze parti, sono quelli presenti nella configurazione standard forniti dalla Funzione IT. La medesima Funzione Data Intelligence Management manutiene e aggiorna un database in cui sono mappati i sistemi a cui le differenti unità organizzative hanno accesso e le credenziali. All'interno del medesimo database sono anche censite le caselle PEC in uso presso la SGR.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT.

11.1.5. Archiviazione della documentazione

L'archiviazione dei documenti in formato elettronico è supportata da specifici applicativi e documentali che permettono il tracciamento degli accessi e la consultazione dei documenti, attraverso meccanismi di *log management*, sia con riferimento ai soggetti che hanno particolari poteri di accesso quali gli amministratori di sistema sia in relazione agli utenti.

La Funzione ha accesso a tutta la documentazione necessaria allo svolgimento delle propria attività istituzionale e tiene traccia degli esiti delle proprie verifiche coerentemente con la metodologia di revisione applicata.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura di revisione interna;
- Policy Trattamento dei dati personali;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Politica di gestione dell'archiviazione.

11.1.6. Gestione del processo di selezione dei fornitori e degli outsourcer

Il conferimento di incarichi a fornitori esterni avviene coerentemente con la struttura di deleghe e poteri basata su tipologie di operazioni, soglie e meccanismi a una o più firme.

A seconda degli importi possono essere invitati 1 o più fornitori di cui viene valutato il possesso dei necessari requisiti alla prestazione del servizio.

La contrattualistica stipulata prevede la possibilità di risoluzione del contratto - fatta salva l'eventuale richiesta di risarcimento – in caso di comportamenti in contrasto con quanto definito nello stesso.

È a cura del richiedente verificare lo stanziamento a budget dell'importo per la specifica attività e fornire i necessari dettagli all'Area Amminitrazione e Controllo affinchè possa proceder con il pagamento delle prestazioni.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura di acquisto di beni e servizi;
- Policy Antiriciclaggio;
- Manuale degli adempimenti antiriciclaggio e per il contrasto al finanziamento del terrorismo (di seguito "Manuale Antiriciclaggio");
- Gestione dei conflitti di interesse;
- Procedura Contabilità.

11.1.7. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

La gestione dei rapporti con la Pubblica Amministrazione prevede il coinvolgimento di diversi Organi e soggetti, anche appartenenti a Aree differenti.

In generale, secondo quanto previsto dal sistema dei poteri e delle deleghe della SGR l'Amministratore Delegato e il Presidente hanno il potere di rappresentare la Società davanti a uffici pubblici e di firmare la corrispondenza.

Ciascun Responsabile, che nell'espletamento delle proprie funzioni intrattenga rapporti con la Pubblica Amministrazione, deve coordinarsi con la Funzione competente nella specifica area d'interesse.

Tutte le comunicazioni pervenute dalla Pubblica Amministrazione sono consegnate al Responsabile della Funzione competente, il quale, valutate le richieste pervenute, ha il compito di richiedere i dati e le informazioni ufficiali alle Aree responsabili e di trasmettere, nel rispetto dei principi di tempestività, correttezza, chiarezza e accuratezza, la documentazione alla Pubblica Amministrazione.

In riferimento a eventuali ispezioni da parte di funzionari pubblici presso la sede sociale, devono presenziare almeno due soggetti della Società. In occasione di ispezioni, i Responsabili delle Funzioni competenti possono avvalersi, se opportuno, di professionisti esterni. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Protocollo corrispondenza in entra ed uscita;
- Procedura Contabilità;
- Politica di gestione dei rapporti con la Pubblica Amministrazione e Autorità di Vigilanza, anche in caso di ispezioni.

11.2. Area controlli

In riferimento all'area Controlli , sono state individuate le seguenti attività sensibili:

- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- gestione dei rapporti con il Collegio Sindacale;
- gestione dei rapporti con la Società di revisione;
- gestione dei reclami;
- gestione degli adempimenti antiriciclaggio e antiterrorismo;
- valutazione del portafoglio degli OICR gestiti;
- gestione dei procedimenti autorizzativi legati all'attività istituzionale, con le Autorità di Vigilanza;
- gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza;
- gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;
- gestione del processo di selezione dei fornitori e di outsourcer;
- accesso al sistema informatico o database di terzi;
- gestione delle operazioni con parti correlate;
- archiviazione della documentazione;

- redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata;
- gestione della contabilità e delle attività funzionali alla predisposizione del bilancio;
- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.2.1. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

La gestione dei rapporti con le Autorità di Vigilanza prevede il coinvolgimento di diversi Organi e soggetti, anche appartenenti a aree differenti.

In generale, secondo quanto previsto dal sistema dei poteri e delle deleghe della SGR l'Amministratore Delegato e il Presidente hanno il potere di rappresentare la SGR davanti a uffici pubblici e di firmare la corrispondenza.

In riferimento a eventuali ispezioni e richieste da parte delle Autorità di Vigilanza, fatte salve diverse e specifiche disposizioni delle Autorità medesime, sono per prassi in essere le seguenti modalità di gestione:

- il responsabile dell'Area controlli è individuato quale referente interno per il coordinamento delle attività connesse alla gestione dei rapporti con i funzionari delle Autorità;
- agli incontri con i funzionari possono partecipare altri soggetti, anche appartenenti ad aree distinte;
- sono previsti momenti di coordinamento e/o allineamento ai quali partecipano le aree/ funzioni/ unità della SGR per le materie di propria competenza;
- le aree/ funzioni/ unità di volta in volta interessate producono le informazioni ed i documenti da fornire, richiesti dalle Autorità, nel rispetto delle previsioni normative applicabili nella materia rilevante, ove necessario avvalendosi del supporto/ coordinamento della funzione Compliance;
- i documenti e le informazioni richiesti sono quindi inviati dalle aree/ funzioni/ unità interessate al CRO, che provvede ad archiviarli in un'area protetta della rete aziendale, appositamente messa a disposizione dell'Autorità.

L'area/ funzione/ unità che produce i documenti e le informazioni da trasmettere archivia gli stessi in formato elettronico, unitamente a eventuali altre evidenze a supporto.

I flussi informativi verso le Autorità e le comunicazioni intercorrenti con i funzionari sono generalmente effettuate tramite posta elettronica/ PEC e, comunque, mediante modalità che ne garantiscono la tracciabilità (es. canali telematici delle Autorità, ricevute di avvenuta trasmissione).

Il Codice Etico e di Comportamento adottato dalla SGR specifica che qualsiasi relazione con le Istituzioni deve svolgersi in maniera trasparente, rigorosa e coerente, nel rispetto della normativa vigente e sulla base di principi di correttezza e lealtà, evitando comportamenti volti a influenzare impropriamente ed indebitamente le attività e le decisioni delle Istituzioni.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Protocollo corrispondenza in entrata ed uscita;
- Politica di gestione dei rapporti con la Pubblica Amministrazione e Autorità di Vigilanza, anche in caso di ispezioni

11.2.2. Gestione dei rapporti con il Collegio Sindacale

Si rinvia al capitolo 11.1.2. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Regolamento del Coniglio di Amministrazione e dei Comitati endo-consiliari.

11.2.3. Gestione dei rapporti con la Società di revisione

Si rinvia al capitolo 11.1.3. per l'analisi dei presidi relativi a tale attività sensibile.

11.2.4. Gestione dei reclami

Le attività connesse alla gestione dei reclami prevedono il coinvolgimento di diverse aree/ unità/ funzioni della SGR. In particolare:

- *Amministratore delegato*: verifica e approva le risposte ai reclami ricevuti e decide in merito al contenuto delle risposte alle ulteriori comunicazioni della clientela;
- *Unità di Compliance*: è responsabile del trattamento dei reclami destinati alla SGR, dell'archiviazione della relativa documentazione e dell'alimentazione e aggiornamento del Registro dei Reclami. L'untà di Compliance tramite il Responsabile dell'Area controlli riferisce al Consiglio di Amministrazione, almeno una volta all'anno, in merito ai rischi individuati e al trattamento dei reclami, nonché alle misure correttive adottate o da adottare. All'unità di Compliance spetta inoltre il compito di sottoporre a verifica la procedura predisposta per il trattamento dei reclami almeno una volta all'anno ovvero in occasione di modifiche normative o organizzative e di proporre eventuali aggiornamenti al Consiglio di Amministrazione;
- *Responsabile dell'Area interessata dal reclamo*: supporta la funzione Compliance nella fase di approfondimento e indagine;
- *Area Legal*: supporta la funzione Compliance nella predisposizione della risposta all'istanza di reclamo.

Si evidenzia che la SGR ha aderito al sistema di risoluzione stragiudiziale delle controversie ACF (Arbitro per le Controversie Finanziarie, istituito presso la Consob).

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura gestione reclami.

11.2.5. Gestione degli adempimenti antiriciclaggio e antiterrorismo

Gli adempimenti collegati a tale attività vedono il coinvolgimento di più soggetti. In particolare:

- l'unità Fund & Client Services esegue l'attività di adeguata verifica della clientela per quanto concerne la raccolta di informazioni e documenti necessari presso i clienti e trasmette all'outsourcer le informazioni relative ai rapporti continuativi e alle operazioni occasionali ai fini della registrazione delle stesse in AUI;
- la funzione Antiriciclaggio effettua le verifiche di secondo livello sull'esecuzione degli adempimenti AML/CFT;
- ogni dipendente della SGR può avviare l'iter di segnalazione di operazione sospetta;

- presso l'outsourcer esterno, in base al relativo contratto di servizio intercorrente con la SGR, è collocato l'AUI.

Nella normativa interna sono definiti i ruoli e le responsabilità dei soggetti che intervengono nelle attività connesse alla gestione degli adempimenti AML/CFT.

Con apposita delibera del Consiglio di Amministrazione, è individuato il responsabile Antiriciclaggio nel responsabile della funzione Antiriciclaggio, pure responsabile delle segnalazioni di operazioni sospette.

Nell'ambito della normativa interna è inoltre definito l'iter per l'invio di segnalazioni di operazioni sospette, il quale può generarsi da parte di tutti i dipendenti della SGR e prevede il coinvolgimento, secondo un meccanismo di escalation, del responsabile gerarchico del soggetto che ha individuato l'operazione sospetta, della funzione Antiriciclaggio e del Delegato SOS.

Le attività di adeguata verifica della clientela e profilatura del rischio sono poste in essere - preliminarmente all'instaurazione del rapporto tra SGR e clienti-investitori - dai soggetti dell'unità Fund & Client Services, tramite la raccolta dei dati e documenti necessari, nonché tramite l'uso di uno strumento operativo (file Excel) che consente di determinare il profilo di rischio all'atto della compilazione del questionario di KYC.

Per i fondi gestiti dalla SGR e domiciliati in Lussemburgo e per i fondi distribuiti da distributori terzi, le attività di adeguata verifica della clientela e di profilatura del rischio vengono svolte da soggetti terzi.

La normativa interna, inoltre, identifica i casi nei quali è prevista l'adeguata verifica rafforzata, che viene effettuata con il supporto necessario della funzione Antiriciclaggio.

Con riferimento agli obblighi di conservazione e registrazione dei dati, l'unità Fund & Client Services verifica, in relazione a ciascuna operazione soggetta a registrazione in AUI da parte dell'outsourcer, la puntualità, la completezza e l'adeguatezza delle registrazioni, comunicando gli esiti di tali verifiche alla funzione Antiriciclaggio.

Con riferimento ai flussi S.AR.A., l'outsourcer trasmette i relativi flussi, secondo tempistiche definite dalla normativa interna e in conformità a quella esterna, in via telematica tramite l'apposito portale fornito dall'AA.VV. Il flusso segnaletico, invece, viene archiviato dall'unità Fund & Client Services.

Con riferimento alla segnalazione delle operazioni sospette, la SGR si è dotata di apposita modulistica ai fini delle relative segnalazioni. Il soggetto segnalante invia la segnalazione al Delegato SOS che, qualora ritenuta fondata, la trasmette all'AA.VV. in via telematica. Lo stesso archivia tutta la documentazione relativa a ciascuna operazione sospetta, anche in caso di mancata trasmissione all'AA.VV. Sono archiviate altresì le comunicazioni eventualmente intercorse con l'AA.VV.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;

- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio.

11.2.6. Valutazione del portafoglio degli OICR gestiti

Nell'ambito delle attività in argomento è previsto il coinvolgimento di più soggetti/ funzioni/ aree/ Organi e altri enti, anche esterni. In particolare la funzione di valutazione dei beni è affidata:

- per i fondi UCITS e i FIA ai depositari;
- per i titoli illiquidi alla funzione Risk Management il cui operato è supervisionato dal Pricing Policy Committee (PPC), La funzione Risk Management, quale funzione indipendente della gestione, supporta inoltre il Consiglio di Amministrazione nell'adozione delle policy di valutazione dei beni e nella loro costante revisione (almeno annuale) in relazione ai titoli in cui i fondi sono investiti.

In relazione ai fondi UCITS ed ai FIA esteri, il depositario affidatario dell'incarico ha assunto la diretta responsabilità in ordine alle conseguenze patrimoniali derivanti da eventuali errori compiuti nel corso dello svolgimento di tale incarico. Lo stesso ha altresì istituito un'unità operativa dedicata, dotata di risorse adeguate, che dispone di sistemi informativo - contabili in grado di assicurare la corretta e tempestiva valorizzazione della quota. Al fine di assicurare la segregazione delle attività, l'unità operativa dedicata alla valorizzazione della quota è organizzata separatamente rispetto a quella preposta all'attività di depositario.

Per i titoli illiquidi, la SGR mette a disposizione del depositario la documentazione, i dati e le informazioni necessari al calcolo del valore della quota.

La trasmissione dei flussi informativi relativi all'ordinaria operatività avviene tramite collegamenti telematici, compresa la posta elettronica, purché documentabile su supporto duraturo. Altre tipologie di comunicazioni sono considerate valide solo se trasmesse per iscritto, a mezzo lettera raccomandata con avviso di ricevimento, via corriere, tramite telefax, telegramma.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;

- Mansionario;
- Policy di Risk Management;
- Procedura di Risk Management;
- Procedure per il monitoraggio del calcolo del NAV;
- Policy violazione limiti di investimento;
- Policy contenenti criteri per la valorizzazione strumenti finanziari OICR;
- Cost transparency_MIFID II.

11.2.7. Gestione dei procedimenti autorizzativi legati all'attività istituzionale con le Autorità di Vigilanza

La gestione dei procedimenti autorizzativi verso le Autorità di Vigilanza prevede il coinvolgimento di diversi Organi e soggetti, anche appartenenti a aree differenti.

Il Consiglio di Amministrazione approva la documentazione e le istanze prima del loro invio, l'Area Controlli supporta l'Area Legal nella predisposizione dei documenti. Tutta la documentazione, nelle varie versioni prodotte, risulta archiviata dall'Area Legal.

Le Aree/unità organizzative coinvolte nel processo di predisposizione forniscono dati e informazioni sempre ricostruibili negli archivi della Società.

In caso di interlocuzioni formali con le Autorità di Vigilanza, sono coinvolti il Presidente o l'Amministratore Delegato che, secondo quanto previsto dal sistema dei poteri e delle deleghe della SGR, hanno il potere di rappresentare la Società davanti a uffici pubblici.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Politica di gestione dei rapporti con la Pubblica Amministrazione e Autorità di Vigilanza, anche in caso di ispezioni.

11.2.8. Gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza

La gestione degli adempimenti informativi verso le Autorità di Vigilanza prevede il coinvolgimento di diversi Organi e soggetti, anche appartenenti ad aree differenti, nonché il supporto di outsourcer. Per ogni tipologia di adempimento la SGR ha individuato un'Area interna resposnabile e definito i ruoli delle altre unità organizzative di supporto.

Con specifico riferimento ai flussi informativi da/verso le Autorità di Vigilanza che vedano coinvolta l'unità di financial Risk Management e di Compliance (es. Relazione annuale della funzione, segnalazioni ai sensi della AIFMD, comunicazioni periodiche alla CSSF):

- è manutenuto uno scadenziario dei principali flussi informativi dovuti alle Autorità, redatto in conformità alle normative di riferimento;
- la funzione Compliance produce e fornisce i contenuti di propria competenza;
- possono essere previsti momenti di condivisione e approvazione con altre aree/ Organi/ funzioni/ unità: in particolare, la Relazione annuale della funzione è portata in approvazione al Consiglio di Amministrazione, dopo aver acquisito il parere del Comitato Controlli Interni e Rischi, e i flussi informativi la cui produzione prevede il coinvolgimento di più aree sono verificati in termini di coerenza e correttezza e completezza in fase di consolidamento delle informazioni da parte del soggetto volta per volta competente.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Comunicazioni e segnalazioni regolamentari;
- Contrattualistica di servizio stipulata con i relativi Outsourcer (previsioni operative).

11.2.9. Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore

L'acquisto e l'utilizzo di software/banche dati deve avvenire con il coinvolgimento dell'Unità Data Intelligence Management che è responsabile del processo di gestione dell'installazione; l'Unità Data Intelligence Management tiene traccia in apposito DataBase degli applicativi in uso, le finalità e le credenziali di accesso.

Specifici controlli attivati sul traffico dati da e verso l'esterno della rete aziendale possono permettere l'individuazione di software installati dagli utenti in maniera non conforme alle regole aziendali.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura acquisto di beni e servizi;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT.

11.2.10. Gestione del processo di selezione dei fornitori e degli outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.2.11. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.2.12. Gestione delle operazioni con parti correlate

La SGR, nell'ambito della gestione dei conflitti di interesse legati alla prestazione dei servizi di investimento e del servizio di gestione collettiva del risparmio individua specifici presidi a tutela dei propri clienti; le parti correlate da cui potrebbe originare un potenziale conflitto di interessi sono oggetto di mappatura dal parte della SGR.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy per la gestione dei conflitti di interesse.

11.2.13. Archiviazione della documentazione

La normativa interna definisce principi generali rispetto alle modalità di archiviazione e gestione del patrimonio informativo aziendale, anche in relazione alla trattatazione di dati personali. In relazione all'accesso a documenti archiviati su sistemi informatici, sono implementati meccanismi di log management. All'interno delle procedure aziendali, ove ritenuto necessario, trovano spazio specifiche indicazioni in merito all'archiviazione di documenti.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Procedura Contabilità;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Policy sul trattamento dei dati personali;
- Politica di gestione dell'archiviazione.

11.2.14. Redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata

La SGR ha definito nelle proprie procedure principi e regole sulle modalità con cui deve fornire in generale informazioni ai propri clienti e regole generale sulle modalità di formalizzazione in apposita documentazione; in relazione all'informativa precontrattuale sono indicate le varie informative che devono essere fornite ai propri clienti.

Specifiche regole di condotta sono inoltre state individuate per la gestione delle informazioni, in particolare quando le stesse assumono la nozione di *privilegiate* nell'ambito della normativa in tema di abusi di mercato.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;

- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy Operazioni personali;
- Procedura Market Abuse;
- Procedura collocamento e prodotti complessi;
- Cost transparency MIFID_II.

11.2.15. Gestione della contabilità e delle attività funzionali alla predisposizione del bilancio

Si rinvia al capitolo 11.3.3. per l'analisi dei presidi relativi a tale attività sensibile.

L'Area Controlli fornisce, in relazione ad alcune fattispecie particolari (ad esempio errori operativi che hanno originato potenziali perdite), indicazioni all'Area Amministrazione e Controllo, in merito alla quantificazione da rappresentare nelle scritture contabili di tali fattispecie. Tali importi sono accompagnati da documenti di analisi che ne supportano sia le modalità di calcolo che le ragioni per la proposta di accantonamento.

11.2.16. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.

11.3. Area Amministrazione e Controllo

In riferimento all'area Amministrazione eControllo, sono state individuate le seguenti attività sensibili:

- gestione degli adempimenti fiscali e delle relazioni con gli Enti Pubblici competenti in materia, anche nel corso di ispezioni;
- gestione della contabilità e delle attività funzionali alla predisposizione del bilancio;
- predisposizione del bilancio di esercizio e dei bilanci intermedi;
- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;

- gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza;
- gestione dei rapporti con la Società di revisione;
- gestione degli adempimenti in materia di tutela ambientale;
- gestione dei c/c della SGR;
- investimenti e operazioni su strumenti finanziari effettuate dalla SGR;
- gestione del processo di selezione dei fornitori e di outsourcer;
- accesso al sistema informatico o database di terzi;
- utilizzo dei meccanismi di firma digitale aziendali;
- archiviazione della documentazione;
- utilizzo delle carte di credito e debito aziendali;
- gestione delle operazioni con parti correlate;
- gestione delle caselle di posta elettronica certificata aziendali;
- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.3.1. Gestione degli adempimenti fiscali e delle relazioni con gli Enti Pubblici competenti in materia, anche nel corso di ispezioni

L'area Amministrazione e Controllo della SGR si avvale per l'attività sensibile in oggetto del supporto di uno studio fiscale-tributario (di seguito il "Fiscalista").

Con specifico riferimento ai dati trasmessi al Fiscalista funzionalmente all'esecuzione degli adempimenti allo stesso affidati, l'area Amministrazione e Controllo:

- effettua un preliminare controllo di conformità sui dati trasmessi (messi a disposizione da Previnet);
- effettua un'ulteriore verifica sulle dichiarazioni predisposte dal Fiscalista, validandone il contenuto prima del materiale invio agli Enti da parte del Fiscalista.

Il sistema contabile in utilizzo consente la tracciabilità dei dati contabili funzionali all'esecuzione degli adempimenti fiscali. Lo stesso sistema permette di allegare a ciascuna registrazione contabile copia elettronica della documentazione a essa collegata (es. fatture, distinte di pagamento). I documenti sono memorizzati negli archivi di gestione documentale presso l'outsourcer amministrativo.

È previsto l'utilizzo della posta elettronica per le comunicazioni tra la Società, il Fiscalista e l'outsourcer amministrativo.

La tracciabilità dei flussi informativi verso l'Agenzia delle Entrate (es. dichiarazioni) è garantita grazie all'utilizzo di dedicati canali telematici di trasmissione, nonché tramite strumenti informatici messi a disposizione dall'Agenzia stessa per la relativa consultazione (es. Cassetto Fiscale).

Inoltre, in generale, la corrispondenza in entrata e in uscita viene protocollata e archiviata dalla Segreteria di Direzione, che provvede ad assegnare una denominazione e ad archiviare in forma cartacea presso l'archivio societario.

Con specifico riferimento alla gestione delle relazioni con Enti Pubblici competenti in materia fiscale, qualsiasi relazione deve svolgersi in maniera trasparente, rigorosa e coerente, nel rispetto della normativa vigente e sulla base di principi di correttezza e lealtà, evitando comportamenti volti a influenzare impropriamente e indebitamente le attività e le decisioni delle Istituzioni. Ai sensi del vigente sistema dei poteri e delle deleghe, l'Amministratore Delegato e il Presidente hanno il potere di rappresentare la Società davanti a uffici finanziari, fiscali e governativi. Infine le comunicazioni intercorrenti con Enti Pubblici sono effettuate tramite posta elettronica e, comunque, mediante sistemi che ne garantiscono la tracciabilità.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy acquisti beni e servizi:
- Controllo e Pagamento delle Commissioni di Gestione e di Performance – Prodotti Gestiti;
- Policy Antiriciclaggio;
- Protocollo corrispondenza in entra ed uscita;
- Gestione dei conflitti di interesse;
- Procedura Contabilità;
- Procedura FATCA.

11.3.2. Gestione della contabilità e delle attività funzionali alla predisposizione del bilancio

L'area Amministrazione e Controllo è competente alla raccolta dei dati funzionali alla redazione del progetto di bilancio e al coordinamento delle attività a ciò propedeutiche.

Sono previste modalità interne e periodiche di trasmissione dei dati necessari all'outsourcer amministrativo, anche per il tramite di più aree della SGR.

Per quanto riguarda i dati specificamente relativi alla contabilità della Società, l'area Amministrazione e Controllo provvede manualmente all'inserimento dei dati all'interno del software gestionale fornito da Previnet.

Il responsabile dell'area Amministrazione e Controllo supervisiona le attività di competenza dell'Area stessa ed è responsabile del presidio dell'operato dell'outsourcer.

Precedentemente all'invio all'outsourcer dei dati contabili relativi ai fondi e della Società, l'area Amministrazione e Controllo svolge un'attività di controllo e quadratura sui medesimi.

L'area Amministrazione e Controllo e l'outsourcer, per gli ambiti di rispettiva competenza, conservano e archiviano, in formato digitale e/o cartaceo le evidenze delle comunicazioni e dei dati in materia contabile.

In generale, inoltre, qualsiasi comunicazione da e verso le strutture coinvolte nell'attività sensibile in esame è effettuata tramite l'utilizzo della posta elettronica o comunque di strumenti che ne garantiscano la tracciabilità.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Contabilità.

11.3.3. Predispsozione del bilancio di esercizio e dei bilanci intermedi

Il Consiglio di Amministrazione delibera in merito al progetto di bilancio, il quale è in ultima istanza approvato dall'Assemblea dei soci. I consiglieri ricevono il progetto utile in anticipo e con congruo anticipo per lo svolgimento delle proprie analisi.

Il responsabile dell'area Amministrazione e Controllo supervisiona le attività di competenza dell'Area stessa ed è responsabile del presidio dell'operato di eventuali outsourcer.

Nelle fasi di chiusura contabile, l'area effettua un'attività di verifica sugli schemi contabili prodotti (destinati a confluire nella documentazione ufficiale relativa alla Società e ai fondi gestiti).

Il Responsabile valida i dati contabili prodotti.

Il progetto di bilancio è sottoposto alle attività di verifica di competenza del Collegio Sindacale.

La Società ha affidato l'incarico di revisione legale ad una Società iscitta in apposito albo, la quale provvede a verificare la regolare tenuta della contabilità sociale e la corretta rilevazione dei fatti di gestione nelle scritture contabili, la coerenza della Relazione sulla gestione con il bilancio d'esercizio e della Relazione degli Amministratori con i Rendiconti di gestione dei fondi. Successivamente, rilascia apposito giudizio.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Contabilità.

11.3.4. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

Si rinvia al capitolo 11.2.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.3.5. Gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza

Nell'ambito delle attività connesse all'effettuazione delle segnalazioni di vigilanza di propria competenza, l'area Amministrazione e Controllo si avvale del supporto di un outsourcer per la prestazione di servizi, tra gli altri, relativi alla gestione amministrativa e contabile dei dati connessi all'operatività della SGR e degli OICR dalla stessa gestiti, inclusi i dati sottostanti alle segnalazioni obbligatorie a cui la SGR stessa è tenuta ai sensi della normativa applicabile.

L'outsourcer supporta altresì la SGR ai fini della produzione e della materiale trasmissione delle segnalazioni, previa validazione da parte dell'area Amministrazione e Controllo.

La Società si è dotata di un elenco interno delle comunicazioni redatto in conformità alle normative di riferimento, relativo all'adempimento di obblighi di segnalazione verso le Autorità di Vigilanza.

Nel rispetto di tale elenco, le competenti aree/ unità della SGR comunicano all'outsourcer (ove non già nella disponibilità dello stesso) i dati e le informazioni rilevanti, relative alla SGR e ai fondi dalla stessa gestiti.

L'outsourcer elabora i dati e le informazioni trasmessigli al fine di predisporre il flusso segnaletico secondo gli schemi previsti da Banca d'Italia, sottoponendolo quindi al controllo automatico del software diagnostico messo a disposizione dell'Autorità. Di seguito, trasmette all'area Amministrazione e Controllo, a mezzo di posta elettronica, la prima bozza di segnalazione con il dettaglio della composizione delle varie poste. Il responsabile verifica la bozza di segnalazione e, se del caso, comunica all'outsourcer, mediante posta elettronica, le eventuali modifiche da apportare. Quest'ultimo recepisce i feedback sottoponendo nuovamente al responsabile dell'area Amministrazione e Controllo la nuova bozza di segnalazione. Terminata la condivisione, il responsabile trasmette il flusso segnaletico definitivo, mediante posta elettronica, all'outsourcer e, in copia conoscenza, all'Amministratore Delegato.

Il materiale invio delle segnalazioni è effettuato dll'Outsourcer, ovvero dall'area Amministrazione e Controllo, nel rispetto dei livelli di servizio contrattualizzati.

In presenza di anomalie afferenti alle segnalazioni, l'outsourcer ne comunica l'oggetto all'area Amministrazione e Controllo e, qualora le anomalie siano effettivamente riscontrare, provvede all'ottenimento della validazione e autorizzazione all'invio da parte dell'Amministratore Delegato.

La documentazione prodotta a supporto delle segnalazioni è archiviata in modalità cartacea, in apposito archivio, e in modalità digitale, su apposita sezione della memoria del server aziendale, a cura del responsabile dell'area Amministrazione e Controllo.

L'outsourcer conserva la documentazione a supporto dell'attività svolta in favore della Società.

La trasmissione delle segnalazioni avviene mediante i canali appositamente messi a disposizione dalle Autorità competenti ed è prodotto e conservato il report di conferma dei flussi trasmessi, a cura dell'Area Amministrazione e Controllo.

Relativamente alla gestione delle comunicazioni verso le Autorità di Vigilanza:

- con riferimento a comunicazioni/documenti ordinariamente previsti ai sensi della normativa applicabile, il responsabile dell'area Amministrazione e Controllo provvede all'invio degli stessi nei tempi e con le modalità previste caso per caso, mentre la funzione Compliance, nell'ambito delle proprie attività di verifica, accerta che l'invio sia effettivamente avvenuto secondo quanto prescritto dalla normativa di riferimento;
- in riferimento, invece, a comunicazioni inerenti a richieste specifiche formulate dalle Autorità, la risposta viene prodotta dalla competente area /unità della SGR;
- qualsiasi comunicazione, prima dell'inoltro alle Autorità, è sottoposta al controllo e successiva approvazione dei soggetti dotati dei necessari poteri di firma;

- in generale, inoltre, il responsabile dell'area Amministrazione e Controllo archivia tutta la documentazione connessa alle comunicazioni in oggetto in apposito archivio cartaceo nonché in modalità digitale, su apposita sezione della memoria del server aziendale.

Con specifico riferimento alla gestione delle relazioni con funzionari delle Autorità di Vigilanza, qualsiasi relazione con le Istituzioni deve svolgersi in maniera trasparente, rigorosa e coerente, nel rispetto della normativa vigente e sulla base di principi di correttezza e lealtà, evitando comportamenti volti a influenzare impropriamente ed indebitamente le attività e le decisioni delle Istituzioni.

Ai sensi del vigente sistema dei poteri e delle deleghe, l'Amministratore Delegato e il Presidente hanno il potere di rappresentare la Società davanti a uffici pubblici.

Le comunicazioni intercorrenti con i funzionari sono effettuate tramite posta elettronica e, comunque, mediante sistemi che ne garantiscono la tracciabilità.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Comunicazioni e segnalazioni regolamentari;
- Contrattualistica di servizio stipulata con i relativi Outsourcer (previsioni operative).

11.3.6. Gestione dei rapporti con la Società di revisione

Si rinvia al capitolo 11.1.3. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario:
- Procedura Contabilità.

11.3.7. Gestione degli adempimenti in materia di tutela ambientale

L'Area Amministrazione e Controllo cura la gestione di limitati adempimenti in tema con il supporto di eventuali fornitori; rilevano allo stato attività di smaltimento di alcune componenti delle stampanti (toner) per cui è stato organizzato un apposito spazio di raccolta che periodicamnete viene svuotato con il supporto della locale azienda di raccolta dei rifiuti e l'eventuale smaltimento di pezzi sostituiti nell'impianto di climatizzazione la cui manutenzione è competenza della SGR, per cui si avvale di azienda specializzata.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Procedura ESG.

11.3.8. Gestione dei c/c della SGR

L'Area Amministrazione e Controllo procede con la predisposizione di mandati di pagamento coerentemente con i poteri di spesa definiti internamente dalla SGR.

Le disposizioni sono predisposte coerentemente con le evidenze documentali che sono poi rappresentate nelle scritture contabili; la documentazione a supporto risulta debitamente archiviata.

Prima di procedere a un pagamento di fornitori viene sempre verificata la rispondenza dell'importo rispetto a quanto contrattualmente previsto e il corretto adempimento della prestazione/consegna dei beni. I conti correnti accesi a nome della SGR sono oggetto di riconciliazione periodica, che risulta adguatamente formalizzata.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura acquisto di beni e servizi;
- Procedura Contabilità.

11.3.9. Investimenti e operazioni su strumenti finanziari effettuate dalla SGR

L'Area Amministrazione e Controllo è responsabile di verificare la presenza di liquidità in eccesso rispetto alle esigenze di cassa nei conti corrente della SGR e comunicarne quindi l'ammontare all'Area Investimenti Fondi Aperti per procedere con l'investimento.

Il responsabile della struttura di *execution* opera coerentemente con le linee guida approvate e riviste periodicamente dal Consiglio di Amministrazione della SGR. Periodicamente i conti deposito intestati alla SGR sono oggetto di apposita riconciliazione, le cui evidenze risultano formalizzate e archiviate.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Contabilità.

11.3.10. Gestione del processi di selezione di fornitori e outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.3.11. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.3.12. Utilizzo dei meccanismi di firma digitale aziendali

È cura dei soggetti che utilizzano meccanismi di firma digitale per conto della SGR accertarsi di avere tutte le necessarie autorizzazioni ad operare.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Politica di gestione della firma digitale.

11.3.13. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile.

11.3.14. Utilizzo delle carte di credito e debito aziendali

La Società, in funzione delle necessità aziendali, ha rilasciato all'Amministratore Delegato e ad alcuni dipendenti le carte di credito con addebito diretto sul c/c aziendale. L'Area Amministrazione e Controllo, nel corso del mese, riceve la nota spese da parte del dipendente a cui è stata rilasciata la carta di credito e dalla Segreteria di Direzione le prenotazioni di voli, hotel, treni e altra documentazione di spese sostenute con la carta di credito aziendale.

L'Amministrazione procede con le opportune registrazioni contabili e, una volta ricevuti gli estratti conto cartacei, effettua le riconciliazioni necessarie.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Procedura Contabilità.

11.3.15. Gestione delle operazioni con parti correlate

Si rinvia al capitolo 11.2.12. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy per la gestione dei conflitti di interesse;
- Procedura Contabilità.

11.3.16. Gestione delle caselle di posta elettronica certificata aziendali

Il responsabile di Funzione/Direzione aziendale, che rilevi l'esigenza di apertura di una nuova PEC dedicata o chiusura di una esistente, può richiedere per mezzo e-mail all'Unità IT, l'attivazione di un nuovo indirizzo PEC; la richiesta deve contenere adeguate motivazioni e i dati relativi agli Utenti abilitati alla fruizione. L'Unità Data Intelligence Management procede alla creazione presso il Fornitore IT del servizio PEC e ne comunica l'avvenuta creazione al Richiedente. Periodicamente, almeno con cadenza annuale, l'Unità Data Intelligence Management verifica, con il Responsabile di Funzione/Direzione che ne usufruisce, la necessità del mantenimento delle caselle e, in caso contrario, provvederà all'eliminazione previa conferma.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT.

11.3.17. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.

11.4. Area HR

In riferimento all'area HR, sono state individuate le seguenti attività sensibili:

- gestione del processo di selezione e assunzione del personale;
- gestione del processo di valutazione, remunerazione e incentivazione del personale;
- organizzazione delle trasferte;
- gestione degli adempimenti in materia di salute e sicurezza nei luoghi lavoro (ex D.Lgs. 81/2008);
- utilizzo dei meccanismi di firma digitale aziendali;

- archiviazione della documentazione;
- utilizzo delle carte di credito e debito aziendali;
- gestione delle caselle di posta elettronica certificata aziendali;
- gestione del processo di selezione dei fornitori e di outsourcer;
- gestione dei rapporti con gli Enti Assistenziali e Previdenziali e altri Enti pubblici (INPS, INAIL, Ispettori del lavoro, Direzione Provinciale del lavoro, Medicina del lavoro, etc.) e degli adempimenti di legge in materia di lavoro e previdenza.

11.4.1. Gestione del processo di selezione e assunzione del personale

Ai sensi del vigente sistema dei poteri e delle deleghe, l'Amministratore Delegato è competente per l'assunzione e il licenziamento del personale dipendente della Società, a esclusione del personale di livello dirigenziale, per il quale la competenza risulta del Consiglio d'Amministrazione.

Il processo di selezione delle risorse umane, nei suoi aspetti di verifica formale e gestione degli adempienti amministrativi, è presidiato dall'area HR.

Nella fase di valutazione dei candidati, sono coinvolti i responsabili delle aree ove origina il fabbisogno di personale.

Una volta ricevuta la richiesta di personale da una struttura interna, l'area HR compie primariamente una verifica di conformità tra il fabbisogno della struttura richiedente e il proprio budget. Ove non sia possibile ricorrere a risorse interne, la stessa approva l'avvio della ricerca dei candidati da parte del Responsabile dell'Area competente, eventualmente mediante il coinvolgimento di società di *recruiting* e *head hunting* al fine di giungere ad una lista di possibili candidati da sottoporre a colloquio.

La valutazione dei candidati avviene mediante colloqui individuali a cura del Responsabile di Area presso cui è aperta la posizione lavorativa per la valutazione di skill tecnici e, in seguito, dell'Amministratore Delegato.

Una volta individuato il potenziale candidato da assumere sulla base dei colloqui effettuati, l'area HR avvia l'iter deliberativo secondo il sistema dei poteri e delle deleghe vigente.

Nel caso di candidati provenienti da paesi terzi, tra i requisiti per la selezione viene considerato il possesso di un regolare permesso di soggiorno; in tale ipotesi, viene effettuato un monitoraggio periodico finalizzato a verificare la validità/scadenza del permesso di soggiorno medesimo.

In generale la selezione del personale è effettuata in base alla corrispondenza dei profili dei candidati e delle loro specifiche competenze alle esigenze aziendali così come formulate dalla funzione richiedente la risorsa e vagliate

dall'Amministratore Delegato e dall'area HR e, in ogni caso, nel rispetto delle pari opportunità per tutti i soggetti interessati.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Gestione delle risorse umane;
- Procedura ESG.

11.4.2. Gestione del processo di valutazione, remunerazione e incentivazione del personale

L'Area HR gestisce il processo di valutazione delle performance dei soggetti interni alla SGR.

La Società ha adottato una politica di remunerazione conforme alla disciplina vigente in materia e applicabile alla SGR. È inoltre istituito il Comitato Remunerazioni.

L'assemblea ordinaria, oltre a stabilire i compensi spettanti agli organi dalla stessa nominati, approva:

- le politiche di remunerazione a favore degli organi con funzione di supervisione, gestione e controllo e del personale;
- i piani basati su strumenti finanziari.

Annualmente il Consiglio di Amministrazione mantiene e riesamina la policy, assicurandosi che il sistema di remunerazione e incentivazione adottato sia coerente con le scelte complessive della SGR in termini di rischi assunti, strategie e obiettivi di lungo termine e con il complessivo assetto di governo societario e dei controlli interni.

La definizione dell'eventuale componente variabile della remunerazione viene svolta avendo cura di non porre obiettivi che non siano raggiungibili tramite una conduzione dell'attività improntata a correttezza e liceità.

Il Comitato Remunerazioni valuta gli aggiornamenti alla policy, assicura il coinvolgimento delle funzioni di controllo nel processo di elaborazione e controllo delle politiche di remunerazione, fornisce consulenza sulla determinazione dei compensi del personale più rilevante, valuta le proposte sui compensi del personale e si esprime sul raggiungimento degli obiettivi di performance da parte delle singole risorse.

L'Area controlli è coinvolta nel processo di definizione e aggiornamento della Policy. Le funzioni di controllo collaborano altresì, ciascuna secondo le rispettive competenze, per assicurare l'adeguatezza e la rispondenza alla normativa della Policy adottata e il suo corretto funzionamento.

Relativamente alle funzioni di controllo:

- l'Area Controlli, attraverso l'unità di Financial e ITC Risk Management valuta, tra l'altro, come la struttura della remunerazione variabile incida sul profilo di rischio della SGR, valutando e convalidando i dati relativi all'aggiustamento per i rischi e partecipando, quando ritenuto opportuno dal RemCo, alle riunioni del Comitato medesimo[9]; tramite la funzione di Compliance verifica, tra l'altro, che il sistema premiante aziendale sia coerente con gli obiettivi di rispetto delle norme, dello statuto, del Codice Etico e di comportamento adottati dalla SGR, in modo che siano opportunamente contenuti i rischi legali e reputazionali insiti soprattutto nelle relazioni con la clientela;
- la Funzione di Internal Audit verifica, tra l'altro, con frequenza almeno annuale, la rispondenza delle prassi di remunerazione alla Policy approvata e alla normativa di riferimento.

Le evidenze riscontrate e le eventuali anomalie sono portate dalle funzioni di controllo a conoscenza dell'organo aziendale competente e del Collegio Sindacale, nonché delle funzioni competenti per l'adozione delle eventuali misure correttive.
Degli esiti delle verifiche condotte è altresì fornita evidenza nelle relazioni delle funzioni di controllo portate annualmente all'attenzione del Consiglio di Amministrazione.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy di remunarazione e incentivazione;
- Gestione delle risorse umane;

[9] Il Chief Risk Officer, ove ritenuto opportuno dal RemCo, partecipa alle relative riunioni soprattutto per assicurare che i sistemi di incentivazione siano adeguatamente corretti per tener conto di tutti i rischi assunti dalla SGR, secondo metodologie coerenti con quelle che la SGR stessa adotta per la gestione dei rischi a fini regolamentari e interni.

- Procedura ESG.

11.4.3. Organizzzazione delle trasferte

L'Area HR supporta nell'organizzazione logistica delle trasferte dei dipendenti, quando autorizzati dai responsabili di area, attraverso l'acquisto diretto dei servizi necessari. Eventuale richieste di rimborso per l'acquisto di beni e servizi nell'ambito di trasferte sono assogettate, previa preliminare autorizzazione del respnsabile di area, a controllo da parte dell'Area Amministrazione e Controllo attraverso la verifica dei giustificativi, prima di procedere con la liquidazione. Il processo risulta tracciato per il tramite di apposito applicativo dedicato.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Proedura Gestione delle risorse umane;
- Procedura Contabilità.

11.4.4. Gestione degli adempimenti in materia di salute e sicurezza nei luoghi lavoro (ex D.Lgs. 81/2008)

Il Responsabile dell'Area HR monitora attraverso incontri periodici con il Responsabile del Servizio di Prevenzione e Protezione - esterno - nominato dalla SGR, la presenza di rischi significativi o problematiche da gestire/indirizzare. In presenza di eventuali problematiche l'Amministratore Delegato è informato al fine di porre in essere in maniera tempestiva gli interventi necessari.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Procedura ESG.

11.4.5. Utilizzo dei meccanismi di firma digitale aziendali

Si rinvia al capitolo 11.3.12 per l'analisi dei presidi relativi a tale attività sensibile.

11.4.6. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile.

11.4.7. Utilizzo delle carte di credito e debito aziendali

Si rinvia al capitolo 11.3.14 per l'analisi dei presidi relativi a tale attività sensibile.

11.4.8. Gestione delle caselle di posta elettronica certificata aziendali

11.4.9. Si rinvia al capitolo 11.3.16 per l'analisi dei presidi relativi a tale attività sensibile.Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.4.10. Gestione dei rapporti con gli Enti Assistenziali e Previdenziali e altri Enti pubblici (INPS, INAIL, Ispettori del lavoro, Direzione Provinciale del lavoro, Medicina del lavoro, etc.) e degli adempimenti di legge in materia di lavoro e previdenza

In merito agli adempimenti amministrativi in materia previdenziale e assistenziale riferiti al rapporto di lavoro dipendente, la Società ha provveduto ad esternalizzarne la gestione ad apposito outsourcer mediante contratto di servizio, che ne specifica ruoli e responsabilità.

L'area HR trasmette periodicamente al consulente del lavoro le informazioni utili per la predisposizione degli adempimenti in materia di lavoro dipendente e previdenza, che poi vengono inseriti nell'applicativo gestionale utilizzato per la contabilità. Dunque, il consulente del lavoro provvede materialmente alla produzione e trasmissione agli Enti competenti della documentazione concernente gli adempimenti in materia di lavoro dipendente e previdenza. A tal fine, il consulente esterno è titolare di deleghe per operare e interfacciarsi direttamente con gli Enti Assistenziali e Previdenziali e gli altri Enti Pubblici competenti.

Il consulente del lavoro, in occasione degli adempimenti annuali e precedentemente al materiale invio di documentazione agli Enti Pubblici competenti, ne trasmette il contenuto alla SGR (area HR) per conferma, che in tale sede effettua controlli a campione sulla correttezza dei dati e delle elaborazioni prodotte dal consulente esterno.

Tutta la documentazione e le evidenze a supporto degli adempimenti posti in essere dall'outsourcer (predisposizione dei cedolini e altri documenti connessi alla posizione assistenziale, previdenziale e fiscale dei lavoratori), è archiviata in formato cartaceo e/o elettronico dall'area HR ovvero dall'outsourcer stesso, per le attività di rispettiva competenza.

Con specifico riferimento alla gestione delle relazioni con Enti Pubblici competenti in materia di lavoro e previdenza, qualsiasi relazione deve svolgersi in maniera trasparente, rigorosa e coerente, nel rispetto della normativa vigente e sulla base di principi di correttezza e lealtà, evitando comportamenti volti a influenzare impropriamente ed indebitamente le attività e le decisioni delle Istituzioni;

Ai sensi del vigente sistema dei poteri e delle deleghe, l'Amministratore Delegato e il Presidente hanno il potere di rappresentare la Società davanti a uffici finanziari, fiscali e governativi. Le comunicazioni intercorrenti con Enti Pubblici sono effettuate tramite posta elettronica e, comunque, mediante sistemi che ne garantiscono la tracciabilità.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Protocollo corrispondenza in entra ed uscita;
- Procedura Contabilità;
- Politica di gestione dei rapporti con la Pubblica Amministrazione e Autorità di Vigilanza, anche in caso di ispezioni.

11.5. Area Legal

In riferimento all'area Legal, sono state individuate le seguenti attività sensibili:

- gestione del contenzioso, giudiziale e stragiudiziale;
- gestione degli adempimenti di segreteria societaria;
- organizzazione e gestione delle riunioni degli organi sociali e tenuta dei libri sociali;
- negoziazione contratti e accordi;
- gestione dei procedimenti autorizzativi legati all'attività istituzionale con le Autorità di Vigilanza;

- utilizzo dei meccanismi di firma digitale aziendali;
- gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza;
- gestione dei reclami;
- gestione del processo di selezione dei fornitori e di outsourcer;
- accesso al sistema informatico o database di terzi;
- archiviazione della documentazione;
- redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata;
- gestione della contabilità e delle attività funzionali alla predisposizione del bilancio;
- gestione delle caselle di posta elettronica certificata aziendali;

11.5.1. Gestione del contenzioso, giudiziale e stragiudiziale

Ai sensi del vigente sistema dei poteri e delle deleghe e della normativa interna:

- all'Amministratore Delegato e al Presidente è conferita la rappresentanza giuridica e giudiziale della Società, nonché la facoltà di nominare procuratori per il compimento di determinati atti o categorie di atti, determinandone gli emolumenti;
- l'Area Legal mantiene e aggiorna il registro dei contenziosi giudiziali e stragiudiziali.

Ai fini della gestione dei contenziosi, la Società si avvale della collaborazione di numerosi studi legali, sulla base di mandati in linea con le condizioni di mercato usualmente praticate, anche in considerazione della specificità dell'incarico e del soggetto coinvolto, nonché del rapporto fiduciario eventualmente stabilito nel tempo con la Società. L'attribuzione degli incarichi di consulenza legale avviene nel rispetto della Procedura "*Procedura selezione e rapporto con outsourcers e fornitori*".

Le attività connesse alla gestione del contenzioso prevedono il coinvolgimento di diverse aree/ unità/ funzioni della SGR. In particolare:

- le attività sono presidiate dall'Area Legal con il supporto della funzione Compliance e delle aree/ unità di volta in volta competenti - eseguono le attività istruttorie, valutando la sussistenza e fondatezza del contenzioso;

- il Consiglio di Amministrazione delibera in merito alle disposizioni di pagamento eventualmente funzionali alla risoluzione del contenzioso. L'esecuzione dell'eventuale pagamento avviene a cura dell'area Amministrazione e Controllo.

Si evidenzia che la SGR ha aderito al sistema di risoluzione stragiudiziale delle controversie ACF (Arbitro per le Controversie Finanziarie, istituito presso la Consob).

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Gestione Reclami.

11.5.2. Gestione degli adempimenti di segreteria societaria

L'Area Legal è responsabile del deposito della documentazione approvata dal Consiglio di Amministrazione o dall'Assemblea degli Azionisti, nei termini previsti dal codice civile, da norme di legge specifiche o dalla regolamentazione di settore.

Tale resposabilità si estende anche all'invio di delibere degli organi sociali all'Autorità di Vigilanza quando richiesto da norme specifiche o su richiesta delle Autorità stesse. L'Area Legal prima della trasmissione/deposito verifica sempre la corrispondenza dell'estratto con quanto contenuto nei libri sociali tenuti dalla SGR.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Procedura Gestione dei conflitti di interesse;
- Mansionario.

11.5.3. Organizzazione e gestione delle riunioni degli organi sociali e tenuta dei libri sociali

L'organizzazione e la gestione delle riunioni degli organi sociali prevede il coinvolgimento di distinti soggetti/ aree/ unità in accordo al Regolamento del fuzionamento degli organi sociali, in particolare:

- il segretario del Consiglio, che cura la predisposizione e la trascrizione dei verbali delle riunioni;
- le aree/ funzioni/ unità della SGR, che predispongono il materiale da portare all'attenzione del Consiglio di Amministrazione, ciascuna per gli ambiti di rispettiva competenza;
- tutti i soggetti convocati alla riunione, ivi compresi i Sindaci.

I documenti sottoposti all'attenzione del Consiglio di Amministrazione sono validati e autorizzati dai soggetti competenti e muniti dei necessari poteri.

Le convocazioni alle riunioni del Consiglio di Amministrazione, a cui partecipa altresì il Collegio Sindacale, sono sottoscritte dal Presidente prima della trasmissione agli Amministratori e ai Sindaci della documentazione.

I verbali delle riunioni del Consiglio di Amministrazione sono approvati dallo stesso nella riunione successiva e sottoscritti dal Presidente per trascrizione nei libri sociali.

Sono definiti e formalizzati specifici iter deliberativi/ autorizzativi per operazioni che presentano profili di conflitti di interesse.

La Segreteria di Direzione monitora l'avvenuta convocazione dei partecipanti alle riunioni del Consiglio di Amministrazione, eventualmente contattando tempestivamente i soggetti che non hanno risposto alla convocazione.

Ai fini di consentire al C.d.A. un adeguato esame degli argomenti all'ordine del giorno delle riunioni, le aree/ funzioni/ unità della SGR interessate trasmettono il materiale a supporto delle stesse al segretario del Consiglio con debito anticipo, per successivo inoltro della documentazione a tutti Consiglieri. Solo in casi di urgenza è possibile far avere ai Consiglieri documentazione con un anticipo inferiore a quello normalmente previsto, comunque motivandone le ragioni.

Il Presidente ed il segretario del Consiglio inviano ai partecipanti alla seduta la bozza del verbale predisposta, ne raccolgono eventuali commenti, apportano eventuali emendamenti e consegnano la versione finale all'area Legal, per trascrizione nei libri sociali previa approvazione alla prima riunione utile del Consiglio di Amministrazione.

Il materiale da portare all'attenzione del C.d.A. in occasione delle relative adunanze è trasmesso ai destinatari (Consiglieri, Sindaci, responsabili di area, etc.) a cura del Segretario tramite una apposita cartella di rete.

Per ogni riunione del C.d.A. è prevista la predisposizione di un verbale a cura del segretario del Consiglio, successivamente inviato ai Consiglieri per relativa condivisione.

I libri sociali e tutti gli allegati sono conservati in appositi armadi di sicurezza.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario
- Policy Gestione dei conflitti di interesse;
- Regolamento del Consiglio di Amministrazione e dei Comitati endo-consiliari;
- Procedura Contabilità.

11.5.4. Negoziazione contratti e accordi

L'Area Legal supporta le altre funzioni aziendali nella stipula degli incarichi con professionisti e in generale nella negoziazione dei contratti quando il mandato è conferito per conto della SGR; in generale assiste i soggetti che lo richiedono nella negoziazione dei contratti, approvandone il contenuto. Entro i termini normativamente previsti redige ed inoltra alle Autorità di Vigilanza le comunicazioni riferite all'esternalizzazione di funzioni aziendali, sottoponendole al CRO per un parere preventivo e all'Amministatore Delegato per la firma; a tal fine le competenti Funzioni aziendali informano l'Area Legal di eventi che diano luogo all'obbligo di comunicazione, eventualmente valendosi della consulenza della funzione del CRO e dell'Area Legal medesima.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy Gestione dei conflitti di interesse;
- Procedura acquisto di beni e servizi;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio;
- Procedura Contabilità.

11.5.5. Gestione dei procedimenti autorizzativi legati all'attività istituzionale con le Autorità di Vigilanza

Si rinvia al capitolo 11.2.7. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.6. Utilizzo dei meccanismi di firma digitale aziendali

Si rinvia al capitolo 11.3.12. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.7. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

Si rinvia al capitolo 11.2.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.8. Gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza

Si rinvia al capitolo 11.3.5. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.9. Gestione dei reclami

Si rinvia al capitolo 11.2.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.10. Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.11. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4 per l'analisi dei presidi relativi a tale attività sensibile.

11.5.12. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.13. Redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata

Si rinvia al capitolo 11.2.14. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.14. Gestione della contabilità e delle attività funzionali alla predisposizione del bilancio

Si rinvia al capitolo 11.3.2. per l'analisi dei presidi relativi a tale attività sensibile.

L'Area Legal, in relazione ad alcune fattispecie particolari (ad esempio contenziosi che possono originare potenziali perdite), fornisce indicazioni all'Area Amministrazione e Controllo, in merito alla quantificazione da rappresentare nelle scritture contabili di tali fattispecie. Tali importi sono accompagnati da documenti di analisi che ne supportano sia le modalità di calcolo che le ragioni per la proposta di accantonamento.

11.5.15. Gestione delle caselle di posta elettronica certificata aziendali

Si rinvia al capitolo 11.3.16. per l'analisi dei presidi relativi a tale attività sensibile.

11.5.16. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.

11.6. Area Data Intelligence Management

In riferimento all'area Data Intelligence Management , sono state individuate le seguenti attività sensibili:

- gestione del processo di selezione dei fornitori e di outsourcer;
- gestione del sistema informativo della Società (ad esempio attraverso: gestione della postazione di lavoro; gestione di accessi verso l'esterno; identificazione di ruoli e procedure con i relativi profili di accesso; installazione di software e contenutii; back up dei dati);

- gestione della sicurezza fisica dei locali, delle relative informazioni e delle apparecchiature;
- accesso al sistema informatico o database di terzi;
- gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;

11.6.1. Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6 per l'analisi dei presidi relativi a tale attività sensibile.

11.6.2. Gestione del sistema informativo della Società (ad esempio attraverso: gestione della postazione di lavoro; gestione di accessi verso l'esterno; identificazione di ruoli e procedure con i relativi profili di accesso; installazione di software e contenuti; back up dei dati)

Il sistema informativo della Società si compone di differenti ambienti operativi, che concorrono all'erogazione dei servizi IT necessari per l'operatività della stessa. In particolare, alcuni dei servizi sono erogati, in funzione di appositi accordi di servizio, attraverso gli outsourcer della Società, i quali garantiscono il possesso di piani di continuità operativa e di sistemi di gestione dei rischi informatici in linea con le esigenze della SGR.

Per ogni processo critico, la Società ha provveduto a identificare distinte risorse che concorrono alla sua esecuzione ed al suo supporto, mediante schede di rilevazione delle responsabilità, delle aree coinvolte, delle procedure informatiche utilizzate e delle infrastrutture necessarie per lo svolgimento delle attività.

Il Consiglio d'Amministrazione della SGR è responsabile dell'identificazione degli obiettivi e delle strategie del piano di continuità operativa e di gestione dei rischi di natura informativa, assicurandone adeguate risorse, tecniche e finanziarie, nonché dell'approvazione del piano di continuità operativa. È invece responsabilità dell'Amministratore Delegato la promozione operativa delle iniziative necessarie affinché il personale della SGR sia adeguatamente informato sulla tematica della continuità operativa ed applichi il relativo piano conformemente a quanto in esso definito.

Il Consiglio di Amministrazione nomina un Crisis Manager, il quale è responsabile dello sviluppo, della manutenzione e delle verifiche di cui al piano di continuità operativa, coordinandosi con il personale coinvolto, per la gestione di tutte le problematiche relative alla continuità operativa della SGR, in riferimento ai rischi di natura informatica e costituito da rappresentanti delle varie strutture aziendali.

La SGR ha adottato una procedura in materia di business continuity e gestione dei rischi informatici, in conformità a quanto definito dai provvedimenti di Banca d'Italia in materia, dunque identificando gli scenari di rischio relativi ai processi critici, le potenziali minacce e le relative contromisure. Inoltre, la Società ha stipulato con un fornitore esterno

un accordo di Disaster Recovery. La predisposizione delle infrastrutture di rete, di provider e dei sistemi di sicurezza informatica viene posta in essere dall'area Data Intelligence Unit.

Al momento dell'assunzione o dell'assegnazione di incarichi a soggetti che agiscano in nome o per conto della Società, è previsto che i candidati, selezionati in relazione all'impiego ed alla sua criticità, sottoscrivano apposite clausole contrattuali di riservatezza delle informazioni e relative alle responsabilità di sicurezza informatica.

L'accesso logico ai sistemi informatici in uso presso la Società avviene esclusivamente tramite sistemi di autenticazione e identificazione che prevedano l'utilizzo di nomi utenti e password personali. L'assegnazione dei profili utente avviene in funzione del ruolo e dell'inquadramento gerarchico del soggetto, al quale sono consentite specifiche tipologie di operatività su dati o documenti informativi.

La funzione Internal Audit ha la responsabilità di controllare l'approccio alla continuità operativa della Società ed il piano di emergenza approvato dal Consiglio d'Amministrazione, partecipando ai test, prendendo visione del piano delle verifiche ed analizzandone i risultati. Inoltre, la funzione Internal Audit estende il proprio controllo agli outsourcer ed ai fornitori critici della SGR, accertandosi che i contratti con gli stessi stipulati tengano conto dei requisiti di sicurezza informativa e di continuità dei processi critici della SGR.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- BCM Plan;
- Policy Trattamento dei dati personali;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT.

11.6.3. Gestione della sicurezza fisica dei locali, delle relative informazioni e delle apparecchiature

L'accesso fisico ai locali della Società avviene tramite meccanismi di riconoscimento (badge) il cui rilascio è tracciato.

In reazione alle informazioni, la SGR assicura il governo della segregazione degli accessi (c.dd. chinese wall) anche a livello logico e funzionale, affinché le informazioni delle varie Funzioni/Direzioni della SGR siano rese accessibili ai soli soggetti che per ruolo devono accedervi, sempre e comunque nel presupposto del principio di "need to know".

Tale segregazione, ottenuta mediante l'applicazione di ruoli, profili e gruppi di appartenenza predefiniti, consente ad ogni Utente di accedere alla documentazione di propria competenza specifica e della conseguente attività lavorativa svolta, garantendo le dovute misure di sicurezza di Trattamento

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- BCM Plan;
- Policy Trattamento dei dati personali;
- Information Technology;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT.

11.6.4. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.6.5. Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore

Si rinvia al capitolo 11.2.9. per l'analisi dei presidi relativi a tale attività sensibile.

11.6.6. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Information Technology;
- Policy sul trattamento dei dati personali;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Politica di gestione dell'archiviazione.

11.7. Area Fund & Client Services

In riferimento all'area Fund & Client Services, sono state individuate le seguenti attività sensibili:

- gestione dei rapporti con la Banca Depositaria;
- gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza;
- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali;
- archiviazione della documentazione;
- gestione del processo di selezione dei fornitori e di outsourcer;
- gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;
- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.7.1. Gestione dei rapporti con la Banca Depositaria

La SGR ha affidato l'incarico di banca depositaria a differenti istituti.

L'unità Fund & Client Services coordina i rapporti con le banche depositarie e mette a disposizione delle stesse i dati e le informazioni necessari per le attività di loro competenza, eventualmente reperendoli presso i competenti outsourcer.

Le competenti aree/ unità della SGR inviano alle banche depositarie la documentazione relativa alle operazioni di investimento autorizzate dal Consiglio di Amministrazione.

In caso di eventuali errori rilevati dalle banche depositarie nel calcolo del net asset value (di seguito anche "NAV"), l'unità Fund & Client Services procede a una nuova verifica del calcolo del valore del NAV, con il supporto dell'outsourcer contabile. Tale verifica avviene tramite un plausibility check, a tendere lo stesso sarà implementato anche sugli OICR italiani. Sono altresì previsti alert automatici in caso di scostamenti del valore del NAV.

I rapporti tra la SGR e le banche depositarie sono regolati da convenzioni scritte e sottoscritte dai soggetti muniti dei necessari poteri. Tali convenzioni definiscono, fra l'altro, le modalità tecniche di scambio dei flussi informativi.

In generale, le comunicazioni tra le banche depositarie e la SGR avvengono a mezzo email.

L'invio della documentazione relativa all'approvazione dell'investimento e alla valorizzazione della quota avviene secondo le modalità tecniche definite nelle convenzioni stipulate tra SGR e banca depositaria.

Generalmente, oltre alla trasmissione dei flussi previsti *ex lege*, la SGR, invia alle banche depositarie la relazione sull'OICR approvata dal C.d.A. e, ove prevista, la relazione della Società di revisione.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedure per il monitoraggio del calcolo del NAV;
- ;
- Policy violazione limiti di investimento;
- Policy contenenti criteri per la vaorizzazione strumenti finanziari OICR.

11.7.2. Gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza

Si rinvia al capitolo 11.3.5. per l'analisi dei presidi relativi a tale attività sensibile.

11.7.3. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

Si rinvia al capitolo 11.2.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.7.4. Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali

La movimentazione dei c/c relativi agli OICR e ai mandati di gestione inidviduale riflette i conferimenti di liquidità, i prelievi di liquidità dei clienti, le operazioni di sottoscrizione e rimborso di quote di OICR e le attività di investimento disposte dale strutture dedicate.

Gli outsourcer amministrativi effettuano periodicamente riconciliazioni della movimentazione dei conti corrente, inviando all'unità Fund & Client Services evdienza delle eventuali discrepanze rilevate così da poter indirizzare, anche verso soggetti esterni, la risoluzione delle eventuali discrepanze.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedure per il monitoraggio del calcolo del NAV;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio.

11.7.5. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Information Technology;

- Policy sul trattamento dei dati personali;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Politica di gestione dell'archiviazione.

11.7.6. Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6 per l'analisi dei presidi relativi a tale attività sensibile.

11.7.7. Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore

Si rinvia al capitolo 11.2.9. per l'analisi dei presidi relativi a tale attività sensibile.

11.7.8. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.

11.8. Area Sales & Marketing

In riferimento all'Area Sales & Marketing, sono state individuate le seguenti attività sensibili:

- stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- accesso al sistema informatico o database di terzi;
- archiviazione della documentazione;

- redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata;
- utilizzo delle carte di credito e debito aziendali;
- gestione del sito internet aziendale;
- utilizzo dei social network;
- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- gestione del processo di selezione dei fornitori e di outsourcer;
- gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;
- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.8.1. Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società

Con specifico riferimento alle fasi operative del processo di collocamento delle quote degli OICR (i.e. promozione di nuovi OICR presso potenziali clienti-investitori, raccolta delle informazioni e della documentazione dai potenziali investitori, verifica del possesso dei requisiti da parte degli stessi e raccolta delle sottoscrizioni, nonché connessi adempimenti normativi, e.g. antiriciclaggio), nell'ambito delle stesse è previsto il coinvolgimento di soggetti/ aree/ unità/ Organi differenti. In particolare:

- l'unità Fund & Client Services:
  - sottopone ai (potenziali) sottoscrittori la documentazione ai sensi della normativa vigente (e.g. informativa precontrattuale, questionario Antiriciclaggio, questionario per la verifica di appropriatezza dell'investimento proposto);
  - valuta l'appropriatezza dell'investimento proposto;
  - archivia le evidenze a supporto delle attività svolte nel processo;
- l'area Legal e la funzione Antiriciclaggio supportano l'unità Fund & Client Services nella predisposizione della documentazione da sottoporre ai (potenziali) sottoscrittori nonché negli adempimenti previsti dalle normative vigenti, comprese le verifiche circa le controparti ai fini antiriciclaggio;

- l'outsourcer effettua le scritture nell'AUI.

L'Area Sales & Marketing supporta il Comitato di Investimenti convocato per la proposta di un nuovo prodotto al C.d.A. ovvero di modifiche significative ai prodotti esistenti. Nel caso in cui un nuovo prodotto e/o prodotto già esistente venga distribuito per il tramite di un altro intermediario, l'unità Fund & Client Services, con il supporto dell'area Legal, predispone con l'intermediario distributore un apposito contratto di distribuzione in cui siano specificati quanto meno i flussi informativi tra la Società e il distributore.

Il Regolamento di gestione degli OICR promossi è approvato dal Consiglio di Amministrazione.

Il modulo di sottoscrizione sottoposto ai potenziali sottoscrittori è sottoscritto dagli stessi e controfirmato per accettazione dall'Amministratore Delegato, previa informativa fornita allo stesso dall'unità Fund & Client Services circa gli esiti delle valutazioni condotte.

Prima di procedere all'esame della posizione di ciascun potenziale sottoscrittore, l'unità Fund & Client Services valuta, sulla base del questionario compilato dal cliente, l'appropriatezza dell'investimento rispetto al profilo del potenziale sottoscrittore, comunicandone allo stesso l'esito.

Ai fini delle verifiche ai sensi della normativa antiriciclaggio, l'unità Fund & Client Services sottopone e raccoglie, insieme alla documentazione prevista, apposito questionario. Le verifiche in oggetto sono espletate con il supporto della funzione Antiriciclaggio, secondo le attività descritte nella normativa interna adottata dalla SGR.

La SGR ha adottato apposite regole per la gestione delle operazioni personali dei Soggetti Rilevanti (come definiti dalla normativa di riferimento) che prevedono:

- che i Soggetti Rilevanti debbano comportarsi con diligenza, correttezza e trasparenza;
- quali operazioni devono essere soggette a un obbligo di segnalazione;
- le responsabilità nella tracciatura di tali operazioni.

La SGR ha inoltre definito nelle proprie procedure principi e regole sulle modalità con cui deve fornire in generale informazioni ai propri clienti e regole generale sulle modalità di formalizzazione in appoita documentazione; in relazione all'informativa precontrattuale sono indicate le varie informative che devono essere fornite ai propri clienti.

Specifiche regole di condotta sono inoltre state individuate per la gestione delle informazioni, in particolare quando le stesse assumono la nozione di privilegiate nell'ambito della normativa in tema di abusi di mercato.

Si evidenzia che la SGR si rivolge soprattutto a investitori istituzionali.

Con riferimento alla corresponsione e percezione degli incentivi, la SGR ha definito specifiche regole per cui è fatto divieto ai Soggetti Rilevanti e ai componenti della struttura organizzativa della SGR di ricevere regali, omaggi e altre utilità se non nel rispetto di quanto previsto dal Codice etico e di Comportamento adottato.

La documentazione relativa agli adempimenti antiriciclaggio espletati è consegnata in originale e in formato elettronico, per archiviazione, al responsabile della funzione Antiriciclaggio.

Sono previste le registrazioni delle operazioni nell'AUI a cura dell'outsourcer amministrativo.

Con generico riferimento alla gestione dei rapporti con i clienti, le comunicazioni ufficiali avvengono tramite mezzi tali da garantirne la tracciabilità (in particolare, e-mail, nelle quali l'Amministratore Delegato è sempre in copia conoscenza). Inoltre, la rendicontazione dei servizi di gestione collettiva prestati a valere sugli OICR sottoscritti avviene mediante la documentazione appositamente prevista ai sensi della normativa vigente in materia.

Anche ai sensi del Codice Etico e di Comportamento, la SGR ha predisposto una specifica policy, nella quale sono indicate le potenziali fattispecie di conflitto di interessi che possono realizzarsi, tenuto conto della sua specifica operatività, le relative misure organizzative e procedurali, nonché i presidi gestionali predisposti al fine di evitare che la presenza dei suddetti conflitti possa ledere gli interessi dei fondi gestiti e degli investitori. La SGR fornisce agli investitori, nell'ambito dell'informativa precontrattuale, una descrizione della propria politica di gestione dei conflitti d'interesse.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy operazioni personali;
-
- Procedura Market Abuse;
- Policy Gestione dei Conflitti di interesse;
- Policy Incentivi;
- Procedura collocamento di OICR e del servizio di gestione di portafogli e distribuzione di prodotti finanziari complessi;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio;
- Cost transparency_MIFID II.

11.8.2. Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento

Con specifico riferimento alle fasi operative del processo di collocamento del servizio di gestione individuale di portafogli e della stipula dell contratto, è previsto il coinvolgimento di soggetti/ aree/ unità/ Organi differenti. In particolare:

- l'unità Fund & Client Services:
  - sottopone ai (potenziali) clienti la documentazione ai sensi della normativa vigente (e.g. informativa precontrattuale, questionario Antiriciclaggio, questionario per la verifica di adeguatezza del servizio proposto);
  - valuta l'adeguatezza del servizio proposto;
  - archivia le evidenze a supporto delle attività svolte nel processo;
- l'area Legal e la funzione Antiriciclaggio supportano l'unità Fund & Client Services nella predisposizione della documentazione da sottoporre ai (potenziali) clienti nonché negli adempimenti previsti dalle normative vigenti, comprese le verifiche circa le controparti ai fini antiriciclaggio;
- l'outsourcer effettua le scritture nell'AUI.

L'Area Sales & Marketing supporta il Comitato di Investimenti convocato per la proposta di un nuova linea / nuovo prodotto al C.d.A. ovvero di modifiche significative a quanto esistente.

Il contratto di gestione sottoposto ai potenziali clienti è sottoscritto dagli stessi e controfirmato per accettazione dall'Amministratore Delegato, previa informativa fornita allo stesso dall'unità Fund & Client Services circa gli esiti delle valutazioni condotte.

Prima di procedere all'esame della posizione di ciascun potenziale cliente, l'unità Fund & Client Services valuta, sulla base del questionario compilato dal cliente, l'adeguatezza del servizio rispetto al profilo del potenziale cliente, comunicandone allo stesso l'esito.

Ai fini delle verifiche ai sensi della normativa antiriciclaggio, l'unità Fund & Client Services sottopone e raccoglie, insieme alla documentazione prevista, apposito questionario. Le verifiche in oggetto sono espletate con il supporto della funzione Antiriciclaggio, secondo le attività descritte nella normativa interna adottata dalla SGR.

La SGR ha adottato apposite regole per la gestione delle operazioni personali dei Soggetti Rilevanti (come definiti dalla normativa di riferimento) che prevedono:

- che i Soggetti Rilevanti debbano comportarsi con diligenza, correttezza e trasparenza;
- quali operazioni devono esseresoggette a un obbligo di segnalazione;
- le responsabilità nella tracciatura di tali operazioni.

La SGR ha inoltre definito nelle proprie procedure principi e regole sulle modalità con cui deve fornire in generale informazioni ai propri clienti e regole generale sulle modalità di formalizzazione in appoita documentazione; in relazione all'informativa precontrattuale sono indicate le varie informative che devono essere fornite ai propri clienti.

Specifiche regole di condotta sono inoltre state individuate per la gestione delle informazioni, in particolare quando le stesse assumono la nozione di privilegiate nell'ambito della normativa in tema di abusi di mercato.

Si evidenzia che la SGR si rivolge soprattutto a investitori istituzionali.

Con riferimento alla corresponsione e percezione degli incentivi, la SGR ha definito specifiche regole per cui è fatto divieto ai Soggetti Rilevanti e ai componenti della struttura organizzativa della SGR di ricevere regali, omaggi e altre utilità se non nel rispetto di quanto previsto dal Codice etico e di Comportamento adottato.

La documentazione relativa agli adempimenti antiriciclaggio espletati è consegnata in originale e in formato elettronico, per archiviazione, al responsabile della funzione Antiriciclaggio.

Sono previste le registrazioni delle operazioni nell'AUI a cura dell'outsourcer amministrativo.

Con generico riferimento alla gestione dei rapporti con i clienti, le comunicazioni ufficiali avvengono tramite mezzi tali da garantirne la tracciabilità (in particolare, e-mail, nelle quali l'Amministratore Delegato è sempre in copia conoscenza). Inoltre, la rendicontazione dei servizi di gestione collettiva prestati a valere sugli OICR sottoscritti avviene mediante la documentazione appositamente prevista ai sensi della normativa vigente in materia.

Anche ai sensi del Codice Etico e di Comportamento, la SGR ha predisposto una specifica policy, nella quale sono indicate le potenziali fattispecie di conflitto di interessi che possono realizzarsi, tenuto conto della sua specifica operatività, le relative misure organizzative e procedurali, nonché i presidi gestionali predisposti al fine di evitare che la presenza dei suddetti conflitti possa ledere gli interessi dei fondi gestiti e degli investitori. La SGR fornisce agli investitori, nell'ambito dell'informativa precontrattuale, una descrizione della propria politica di gestione dei conflitti d'interesse.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy operazioni personali;
- Policy Gestione dei Conflitti di interesse;
- Policy Incentivi;

- Procedura Market Abuse;
- Procedura collocamento di OICR e del servizio di gestione di portafogli e distribuzione di prodotti finanziari complessi;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio;
- Cost transparency MIFID_II.

11.8.3. Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni

Le fattispecie in oggetto sono:

- gestite nel rispetto dei poteri di spesa definiti dalla Società e nell'ambito della gestione del processo di budget e controllo;
- erogate coerentemente con i principi etici e comportamentali definiti dalla SGR.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy Incentivi;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio;
- Policy acquisti beni e servizi;
- Procedura Contabilità.

11.8.4. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.8.5. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Policy Information Technology;
- sul trattamento dei dati personali;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Politica di gestione dell'archiviazione.

11.8.6. Redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata

Si rinvia al capitolo 11.2.14. per l'analisi dei presidi relativi a tale attività sensibile.

11.8.7. Utilizzo delle carte di credito e debito aziendali

Si rinvia al capitolo 11.3.14. per l'analisi dei presidi relativi a tale attività sensibile.

11.8.8. Gestione del sito internet aziendale

Le modalità di aggiornamento e l'approvazione dei contenuti è disciplinata da specifiche regole. La SGR ha inoltre definito nelle proprie procedure principi e regole sulle modalità con cui deve fornire in generale informazioni ai propri clienti e regole generale sulle modalità di formalizzazione in apposita documentazione; in relazione all'informativa precontrattuale sono indicate le varie informative che devono essere fornite ai propri clienti.

Specifiche regole di condotta sono inoltre state individuate per la gestione delle informazioni, in particolare quando le stesse assumono la nozione di privilegiate nell'ambito della normativa in tema di abusi di mercato.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura per l'aggiornamento e il mantenimento del sito web;
- Procedura Market Abuse.

11.8.9. Gestione del social network

Specifiche regole di condotta sono state individuate per la gestione delle informazioni, in particolare quando le stesse assumono la nozione di privilegiate nell'ambito della normativa in tema di abusi di mercato.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Procedura Market Abuse.

11.8.10. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

Si rinvia al capitolo 11.2.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.8.11. Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.8.12. Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore

Si rinvia al capitolo 11.2.9. per l'analisi dei presidi relativi a tale attività sensibile.

11.8.13. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

11.9. Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.Aree Investimenti Fondi Aperti

In riferimento all'Area Investimento Fondi aperti, sono state individaute le seguenti attività sensibili:

- acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi a oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi a oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, e stipulazione di strumenti derivati non negoziati su mercati regolamentati italiani ed europei;
- gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali;
- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- accesso al sistema informatico o database di terzi;
- negoziazione delle condizioni economiche dei servizi esecutivi con le controparti;
- gestione delle operazioni con parti correlate;
- archiviazione della documentazione;
- redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata;
- gestione del processo di selezione dei fornitori e di outsourcer;
- gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;
- investimenti e operazioni su strumenti finanziari effettuate dalla SGR;
- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.9.1. Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli)

Tale attività sensibile prevede il coinvolgimento di diversi soggetti/ aree/ unità/ funzioni/ Organi, anche esterni alla Società. In particolare:

- il C.d.A. è l'organo che approva le linee guida e l'allocazione strategica di ciascun portafoglio, generalmente su proposte avanzate dal Comitato Investimenti; inoltre approva preventivamente o ratifica successivamente le operazioni di investimento e disinvestimento dei portafogli eseguite in deroga a quanto disposto dallo stesso; il C.d.A. verifica la corretta applicazione delle disposizioni e dei principi stabiliti nella presente procedura con cadenza almeno annuale;
- l'Amministratore Delegato è munito di deleghe specifiche e coordina, insieme ai responsabili, ma senza esenzione di responsabilità per i responsabili delle aree investimenti, tutti gli investimenti;
- il Comitato Investimenti è l'organo che assume le decisioni collegiali relative a tutte le risorse dedicate agli investimenti, propone al Consiglio di Amministrazione le linee guida e le allocazioni strategiche e, all'interno del perimetro definito dal C.d.A., approva le allocazioni tattiche;
- il Presidente del Comitato Investimenti riferisce con cadenza periodica al Consiglio di Amministrazione sulle attività di investimento attraverso la trasmissione dei verbali del Comitato medesimo corredati da una breve relazione di sintesi;
- il Comitato Investimenti convocato in forma allargata valuta e approva e modifica le proposte per la creazione, modifica, dismissione di nuovi prodotti o prodotti esistenti, in linea con le linee strategiche definite;
- il responsabile dell'Area riporta all'Amministratore Delegato, i quali coordinano e dirigono le attività dell'area di propria competenza;
- l'Area ha le competenze per gestire tutte le fasi del ciclo di investimenti dei portafogli;
- ciascun componente dell'Area, conformemente alla propria mansione, seniority e competenza, ha il dovere di seguire il presente Modello e le altre norme interne della SGR a questi applicabile (i componenti a cui venga affidata la gestione di un portafoglio di seguito definiti "gestori");
- la funzione di Financial e ITC Risk Management fornisce supporto al Comitato Investimenti e al C.d.A. nella determinazione del profilo di rischio di ogni nuovo OICR, ovvero in fase di revisione periodica, nonché del relativo sistema di limiti; verifica nel continuo sia *ex ante* che *ex post* il rispetto di tali limiti;

- l'Amministratore Delegato e il Comitato Investimenti monitorano costantemente l'attuazione degli indirizzi e delle strategie stabiliti dal Consiglio di Amministrazione e il rispetto della politica di gestione definita nel Regolamento dei Fondi, riferendo in proposito al Consiglio di Amministrazione.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Processo di investimento fondi aperti, GP e pools non delegati;
- Strategia di trasmissione ed esecuzione degli ordini;
- Partecipazioni rilevanti e asset stripping;
- Policy violazione limiti investimento;
- Policy per la gestione dei conflitti di interesse;
- Policy Operazioni personali;
- Procedura Market Abuse;
- Cost transparency_MIFID II .

11.9.2. Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, e stipulazione di strumenti derivati non negoziati su mercati regolamentati italiani ed europei

Tale attività sensibile prevede il coinvolgimento di diversi soggetti/ aree/ unità/ funzioni/ Organi, anche esterni alla Società. In particolare:

- il C.d.A. è l'organo che approva le linee guida e l'allocazione strategica di ciascun portafoglio, generalmente su proposte avanzate dal Comitato Investimenti; inoltre approva preventivamente o ratifica successivamente le operazioni di investimento e disinvestimento dei portafogli eseguite in deroga a quanto disposto dallo stesso; il C.d.A. verifica la corretta applicazione delle disposizioni e dei principi stabiliti nella presente procedura con cadenza almeno annuale;

- l'Amministratore Delegato è munito di deleghe specifiche e coordina, insieme ai responsabili, ma senza esenzione di responsabilità per i responsabili delle aree investimenti, tutti gli investimenti;
- il Comitato Investimenti è l'organo che assume le decisioni collegiali relative a tutte le risorse dedicate agli investimenti, propone al Consiglio di Amministrazione le linee guida e le allocazioni strategiche e, all'interno del perimetro definito dal C.d.A., approva le allocazioni tattiche;
- il Presidente del Comitato Investimenti riferisce con cadenza periodica al C.d.A. sulle attività di investimento attraverso la trasmissione di una breve relazione di sintesi delle delibere del Comitato medesimo;
- il Comitato Investimenti convocato in forma allargata valuta e approva e modifica le proposte per la creazione, modifica, dismissione di nuovi prodotti o prodotti esistenti, in linea con le linee strategiche definite;
- il responsabile dell'Area riporta all'Amministratore Delegato, i quali coordinano e dirigono le attività dell'area di propria competenza;
- l'Area ha le competenze per gestire tutte le fasi del ciclo di investimenti dei portafogli;
- ciascun componente dell'Area, conformemente alla propria mansione, seniority e competenza, ha il dovere di seguire la presente procedura e le altre norme interne della SGR a questi applicabile (i componenti a cui venga affidata la gestione di un portafoglio di seguito definiti "gestori");
- la funzione di Financial e ITC Risk Management fornisce supporto al Comitato Investimenti e al C.d.A. nella determinazione del profilo di rischio di ogni nuovo OICR, ovvero in fase di revisione periodica, nonché del relativo sistema di limiti; verifica nel continuo sia *ex ante* che *ex post* il rispetto di tali limiti;
- l'Amministratore Delegato e il Comitato Investimenti monitorano costantemente l'attuazione degli indirizzi e delle strategie stabiliti dal Consiglio di Amministrazione e il rispetto della politica di gestione definita nei Regolamento dei Fondi, riferendo in proposito al Consiglio di Amministrazione.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Processo di investimento fondi aperti, GP e pools non delegati;
- Strategia di trasmissione ed esecuzione degli ordini;
- Partecipazioni rilevanti e asset stripping;

- Policy violazione limiti investimento;
- Policy per la gestione dei conflitti di interesse;
- Policy Operazioni personali;
- Procedura Market Abuse;
- Cost transparency_MIFID II .

11.9.3. Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali

Si rinvia al capitolo 11.7.4. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy violazione limiti investimento;
-
- Procedura Market Abuse;
- Procedure per il monitoraggio del calcolo del NAV;
- Cost transparency_MIFID II .

11.9.4. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

Si rinvia al capitolo 11.2.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.9.5. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.9.6. Negoziazione delle condizioni economiche dei servizi esecutivi con le controparti

Con riferimento all'attività di negoziazione delle condizioni economiche (commissioi e altri oneri di negoziazione) dei servizi di investimento e gestione del risparmio, la Società prevede l'applicazione di definite regole in tema di incentivi.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy Incentivi;
- Strategia di trasmissione ed esecuzione degli ordini;
- Cost transparency_MIFID II .

11.9.7. Gestione delle operazioni con parti correlate

Si rinvia al capitolo 11.2.12. per l'analisi dei presidi relativi a tale attività sensibile.

11.9.8. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Information Technology;
- Policy sul trattamento dei dati personali;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Politica di gestione dell'archiviazione.

11.9.9. Redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata

Si rinvia al capitolo 11.2.14. per l'analisi dei presidi relativi a tale attività sensibile.

11.9.10. Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.9.11. Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore

Si rinvia al capitolo 11.2.9. per l'analisi dei presidi relativi a tale attività sensibile.

11.9.12. Investimenti e operazioni su strumenti finanziari effettuate dalla SGR

Si rinvia al capitolo 11.3.9. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Cost transparency_MIFID II .

11.9.13. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.

11.10. Aree Investimenti Fondi Chiusi

In riferimento all'Area Investimenti Fondi Chiusi, sono state individaute le seguenti attività sensibili:

- acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli);
- acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi a oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, e stipulazione di strumenti derivati non negoziati su mercati regolamentati italiani ed europei;
- gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti (owner delle Società) con cui sono realizzate le operazioni di investimento e disinvestimento del patrimonio dei Fondi gestiti (a titolo esemplificativo, operazioni di compravendita di quote e azioni di società e di veicoli di investimento non quotate/i);
- gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali;
- gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni;
- accesso al sistema informatico o database di terzi;
- negoziazione delle condizioni economiche dei servizi esecutivi con le controparti;
- gestione delle operazioni con parti correlate;
- archiviazione della documentazione;
- redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata;
- gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza;
- stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società;
- gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento;
- gestione delle caselle di posta elettronica certificata aziendali;
- gestione del processo di selezione dei fornitori e di outsourcer;
- gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore;

- gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni.

11.10.1. Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari quotati relativamente ai patrimoni in gestione (OICR e gestione individuale di portafogli)

Tale attività sensibile prevede il coinvolgimento di diversi soggetti/ aree/ unità/ funzioni/ Organi, anche esterni alla Società. In particolare:

- il C.d.A. è l'organo che approva le linee guida e l'allocazione strategica di ciascun portafoglio, generalmente su proposte avanzate dal Comitato Investimenti; inoltre approva preventivamente o ratifica successivamente le operazioni di investimento e disinvestimento dei portafogli eseguite in deroga a quanto disposto dallo stesso; il C.d.A. verifica la corretta applicazione delle disposizioni e dei principi stabiliti nella presente procedura con cadenza almeno annuale;
- l'Amministratore Delegato è munito di deleghe specifiche e coordina, insieme ai responsabili, ma senza esenzione di responsabilità per i responsabili delle aree investimenti, tutti gli investimenti;
- il Comitato Investimenti è l'organo che assume le decisioni collegiali relative a tutte le risorse dedicate agli investimenti, propone al C.d.A. le linee guida ed le allocazioni strategiche e, all'interno del perimetro definito dal C.d.A., approva le allocazioni tattiche;
- il Presidente del Comitato Investimenti riferisce con cadenza periodica al C.d.A. sulle attività di investimento attraverso la trasmissione di una breve relazione di sintesi delle delibere del Comitato medesimo;
- il Comitato Investimenti convocato in forma allargata valuta e approva e modifica le proposte per la creazione, modifica, dismissione di nuovi prodotti o prodotti esistenti, in linea con le linee strategiche definite;
- il responsabile dell'Area riporta all'Amministratore Delegato, i quali coordinano e dirigono le attività dell'area di propria competenza;
- l'Area ha le competenze per gestire tutte le fasi del ciclo di investimenti dei portafogli;
- ciascun componente dell'Area, conformemente alla propria mansione, seniority e competenza, ha il dovere di seguire la presente procedura e le altre norme interne della SGR a questi applicabile (i componenti a cui venga affidata la gestione di un portafoglio di seguito definiti "gestori");
- la funzione di Financial e ITC Risk Management fornisce supporto al Comitato Investimenti e al C.d.A. nella determinazione del profilo di rischio di ogni nuovo OICR, ovvero in fase di revisione periodica, nonché del relativo sistema di limiti; verifica nel continuo sia *ex ante* che *ex post* il rispetto di tali limiti;

- l'Amministratore Delegato e il Comitato Investimenti monitorano costantemente l'attuazione degli indirizzi e delle strategie stabiliti dal Consiglio di Amministrazione e il rispetto della politica di gestione definita nei Regolamento dei Fondi, riferendo in proposito al Consiglio di Amministrazione.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Processo di investimento fondi chiusi;
- Strategia di trasmissione ed esecuzione degli ordini;
- Partecipazioni rilevanti e asset stripping;
- Policy violazione limiti investimento;
- Policy per la gestione dei conflitti di interesse;
- Policy Operazioni personali;
- Procedura Market Abuse;
- Cost transparency_MIFID II .

11.10.2. Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, e stipulazione di strumenti derivati non negoziati su mercati regolamentati italiani ed europei

Tale attività sensibile prevede il coinvolgimento di diversi soggetti/ aree/ unità/ funzioni/ Organi, anche esterni alla Società. In particolare:

- il C.d.A. è l'organo che approva le linee guida e l'allocazione strategica di ciascun portafoglio, generalmente su proposte avanzate dal Comitato Investimenti; inoltre approva preventivamente o ratifica successivamente le operazioni di investimento e disinvestimento dei portafogli eseguite in deroga a quanto disposto dallo stesso; il C.d.A. verifica la corretta applicazione delle disposizioni e dei principi stabiliti nella presente procedura con cadenza almeno annuale;

- l'Amministratore Delegato è munito di deleghe specifiche e coordina, insieme ai responsabili, ma senza esenzione di responsabilità per i responsabili delle aree investimenti, tutti gli investimenti;
- il Comitato Investimenti è l'organo che assume le decisioni collegiali relative a tutte le risorse dedicate agli investimenti, propone al C.d.A. le linee guida e le allocazioni strategiche e, all'interno del perimetro definito dal C.d.A., approva le allocazioni tattiche;
- il Presidente del Comitato Investimenti riferisce con cadenza periodica al C.d.A. sulle attività di investimento attraverso la trasmissione di una breve relazione di sintesi delle delibere del Comitato medesimo;
- il Comitato Investimenti convocato in forma allargata valuta e approva e modifica le proposte per la creazione, modifica, dismissione di nuovi prodotti o prodotti esistenti, in linea con le linee strategiche definite;
- il responsabile dell'Area riporta all'Amministratore Delegato, i quali coordinano e dirigono le attività dell'area di propria competenza;
- l'Area ha le competenze per gestire tutte le fasi del ciclo di investimenti dei portafogli;
- ciascun componente dell'Area, conformemente alla propria mansione, seniority e competenza, ha il dovere di seguire la presente procedura e le altre norme interne della SGR a questi applicabile (i componenti a cui venga affidata la gestione di un portafoglio di seguito definiti "gestori");
- la funzione di Financial e ITC Risk Management fornisce supporto al Comitato Investimenti e al C.d.A. nella determinazione del profilo di rischio di ogni nuovo OICR, ovvero in fase di revisione periodica, nonché del relativo sistema di limiti; verifica nel continuo sia *ex ante* che *ex post* il rispetto di tali limiti;
- l'Amministratore Delegato ed il Comitato Investimenti monitorano costantemente l'attuazione degli indirizzi e delle strategie stabiliti dal Consiglio di Amministrazione e il rispetto della politica di gestione definita nei Regolamento dei Fondi, riferendo in proposito al Consiglio di Amministrazione.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e didi Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Processo di investimento fondi chiusi;
- Strategia di trasmissione ed esecuzione degli ordini;
- Partecipazioni rilevanti e asset stripping;

- Policy violazione limiti investimento;
- Policy per la gestione dei conflitti di interesse;
- Policy Operazioni personali;
- Procedura Market Abuse;
- Cost transparency_MIFID II .

11.10.3. Gestione delle attività connesse all'investimento del patrimonio degli OICR con particolare riferimento alla gestione dei rapporti con le controparti (owner delle Società) con cui sono realizzate le operazioni di investimento e disinvestimento del patrimonio dei Fondi gestiti (a titolo esemplificativo, operazioni di compravendita di quote e azioni di società e di veicoli di investimento non quotate/i)

Il processo di investimenti prevede una codificata serie di passaggi e l'attribuzione di specifiche responsabilità (cfr. 11.10.1. e 11.10.2.).

La valutazione delle controparti nelle transazioni che hanno ad oggetto società non quotate, quando non avvengono per il tramite di intermediari ablitati, seguono regole di valutazione che contemplano sia tematiche di natura reputazionale che più in generale i controlli antiriciclaggio, per quanto applicabli (ad esempio in tema di segnalazione operazione sospette).

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Processo di investimento fondi chiusi;
- Strategia di trasmissione ed esecuzione degli ordini;
- Partecipazioni rilevanti e asset stripping;
- Policy per la gestione dei conflitti di interesse;
- Policy Operazioni personali;

- Procedura Market Abuse;
- Policy Antiriciclaggio;
- Manuale Antiriciclaggio;
- Cost transparency_MIFID II .

11.10.4. Gestione dei c/c degli OICR gestiti e dei c/c collegati alle gestioni individuali

Si rinvia al capitolo 11.7.4. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Processo degli investimenti fondi chiusi;
- Procedura Market Abuse;
- Procedure per il monitoraggio del calcolo del NAV.

11.10.5. Gestione dei rapporti con le Autorità di Vigilanza, anche nel caso di ispezioni

Si rinvia al capitolo 11.2.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.6. Accesso al sistema informatico o database di terzi

Si rinvia al capitolo 11.1.4. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.7. Negoziazione delle condizioni economiche dei servizi esecutivi con le controparti

Con riferimento all'attività di negoziazione delle condizioni economiche (commissioi e altri oneri di negoziazione) dei servizi di investimento e gestione del risparmio, la Società prevede l'applicazione di definite regole in tema di incentivi.

Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Mansionario;
- Policy Incentivi;
- Strategia di trasmissione ed esecuzione degli ordini;
- Cost transparency_MIFID II .

11.10.8. Gestione delle operazioni con parti correlate

Si rinvia al capitolo 11.2.12. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.9. Archiviazione della documentazione

Si rinvia al capitolo 11.2.13. per l'analisi dei presidi relativi a tale attività sensibile. Tra i principali protocolli e documenti che contengono specifici presidi sul tema si rimanda a:

- Codice Etico e di Comportamento;
- Sistema dei poteri e delle deleghe;
- Relazione sulla struttura organizzativa e sull'assetto contabile;
- Information Technology;
- Policy sul trattamento dei dati personali;
- Politica di gestione dei rischi ICT;
- Manuale Sistemi IT;
- Politica di gestione dell'archiviazione.

11.10.10. Redazione di documenti informativi, prospetti informativi, relazioni, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e/o i prodotti gestiti e i

servizi offerti, destinati alle Autorità di Vigilanza e Controllo oppure agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale, per legge o per decisione della Società, nonché formazione di ogni informazione privilegiata

Si rinvia al capitolo 11.2.14. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.11. Gestione degli adempimenti informativi (ivi comprese le attivite legate alla predisposizione delle segnalazioni di vigilanza per la SGR o per gli OICR gestiti) nei confronti di Autorità di Vigilanza

Si rinvia al capitolo 11.3.5. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.12. Stipula e gestione dei rapporti con la clientela, rappresentata dai sottoscrittori delle quote degli OICR gestiti dalla Società

Si rinvia al capitolo 11.8.1. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.13. Gestione dei rapporti con i (potenziali) clienti-investitori nell'ambito della prestazione di servizi di investimento

Si rinvia al capitolo 11.8.2. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.14. Gestione delle caselle di posta elettronica certificata aziendali

Si rinvia al capitolo 11.3.16. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.15. Gestione del processo di selezione dei fornitori e di outsourcer

Si rinvia al capitolo 11.1.6. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.16. Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altro prodotto tutelato da diritto di autore

Si rinvia al capitolo 11.2.9. per l'analisi dei presidi relativi a tale attività sensibile.

11.10.17. Gestione dei rapporti con la Pubblica Amministrazione, anche nel caso di ispezioni

Si rinvia al capitolo 11.1.7. per l'analisi dei presidi relativi a tale attività sensibile.