



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

INDICE

CAPITOLO 1 - IL CONTESTO NORMATIVO.....	5
1.1 IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO DAL DECRETO LEGISLATIVO N. 231/01 A CARICO DELLE PERSONE GIURIDICHE, SOCIETÀ ED ASSOCIAZIONI	5
1.2 L'ADOZIONE DEI MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALI ESIMENTI DELLA RESPONSABILITÀ AMMINISTRATIVA DELL'ENTE.....	6
CAPITOLO 2 - IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI FIDEURAM INVESTIMENTI SGR S.P.A.....	8
2.1 GLI STRUMENTI AZIENDALI ESISTENTI QUALI PRESUPPOSTI DEL MODELLO	8
2.1.1 <i>Codice Etico e Codice Interno di Comportamento di Gruppo</i>	9
2.1.2 <i>Le caratteristiche salienti del sistema dei controlli interni</i>	10
2.1.3 <i>Il sistema dei poteri e delle deleghe</i>	12
2.2 LE FINALITÀ PERSEGUITE CON L'ADOZIONE DEL MODELLO	13
2.3 GLI ELEMENTI FONDAMENTALI DEL MODELLO.....	14
2.4 LA STRUTTURA DEL MODELLO	15
2.5 I DESTINATARI DEL MODELLO.....	16
2.6 ADOZIONE, EFFICACE ATTUAZIONE E MODIFICAZIONE DEL MODELLO – RUOLI E RESPONSABILITÀ	17
2.7 ATTIVITÀ OGGETTO DI OUTSOURCING	22
2.8 IL RUOLO DELLA CAPOGRUPPO E DELLA CONTROLLANTE FIDEURAM – INTESA SANPAOLO PRIVATE BANKING	23
2.8.1 <i>Principi di indirizzo di Gruppo in materia di Responsabilità amministrativa degli Enti</i>	23
CAPITOLO 3 - L'ORGANISMO DI VIGILANZA.....	27
3.1 INDIVIDUAZIONE DELL'ORGANISMO DI VIGILANZA.....	27
3.2 COMPOSIZIONE, FUNZIONAMENTO E COMPENSI DELL'ORGANISMO DI VIGILANZA	27
3.3 REQUISITI DI ELEGGIBILITÀ, CAUSE DI DECADENZA E SOSPENSIONE.....	28
3.3.1 <i>Requisiti di professionalità, onorabilità ed indipendenza</i>	28
3.3.2 <i>Verifica dei requisiti</i>	29
3.3.3 <i>Cause di decadenza</i>	29
3.3.4 <i>Cause di sospensione</i>	30
3.4 TEMPORANEO IMPEDIMENTO DI UN COMPONENTE EFFETTIVO	32
3.5 COMPITI DELL'ORGANISMO DI VIGILANZA	32
3.6 MODALITÀ E PERIODICITÀ DI RIPORTO AGLI ORGANI SOCIETARI.....	34
CAPITOLO 4 - FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA.....	35
4.1 FLUSSI INFORMATIVI DA EFFETTUARSI AL VERIFICARSI DI PARTICOLARI EVENTI	35
4.2 FLUSSI INFORMATIVI PERIODICI.....	36
CAPITOLO 5 - IL SISTEMA SANZIONATORIO	40
CAPITOLO 6 - FORMAZIONE E COMUNICAZIONE INTERNA	44
6.1 COMUNICAZIONE INTERNA.....	44
6.2 FORMAZIONE	45
CAPITOLO 7 – GLI ILLECITI PRESUPPOSTO - AREE, ATTIVITÀ E RELATIVI PRINCIPI DI COMPORTAMENTO E DI CONTROLLO.....	47
7.1 INDIVIDUAZIONE DELLE AREE SENSIBILI	47
7.2 AREA SENSIBILE CONCERNENTE I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE	48
7.2.1 <i>Fattispecie di reato</i>	48
7.2.2 <i>Attività aziendali sensibili</i>	53
7.2.2.1. <i>Stipula dei rapporti contrattuali con la Pubblica Amministrazione</i>	55
Premessa.....	55
Descrizione del processo.....	55
Principi di controllo.....	56
Principi di comportamento	58
7.2.2.2. <i>Gestione dei rapporti contrattuali con la Pubblica Amministrazione</i>	61
Premessa.....	61
Descrizione del processo.....	61
Principi di controllo.....	62
Principi di comportamento	63

7.2.2.3. Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione	66
Premessa.....	66
Descrizione del processo.....	67
Principi di controllo.....	67
Principi di comportamento.....	69
7.2.2.4. Gestione dei contenziosi e degli accordi transattivi.....	71
Premessa.....	71
Descrizione del processo.....	72
Principi di controllo.....	73
Principi di comportamento.....	74
7.2.2.5. Gestione dei rapporti con le Autorità di Vigilanza.....	77
Premessa.....	77
Descrizione del processo.....	78
Principi di controllo.....	78
Principi di comportamento.....	80
7.2.2.6. Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali	82
Premessa.....	82
Descrizione del processo.....	83
Principi di controllo.....	83
Principi di comportamento.....	85
7.2.2.7. Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni	88
Premessa.....	88
Descrizione del processo.....	89
Principi di controllo.....	90
Principi di comportamento.....	91
7.2.2.8. Gestione del processo di selezione e assunzione del personale.....	94
Premessa.....	94
Descrizione del processo.....	95
Principi di controllo.....	95
Principi di comportamento.....	96
7.3 AREA SENSIBILE CONCERNENTE I REATI SOCIETARI	98
7.3.1 Fattispecie di reato.....	98
7.3.2 Attività aziendali sensibili.....	103
7.3.2.1. Gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione	105
Premessa.....	105
Descrizione del processo.....	105
Principi di controllo.....	106
Principi di comportamento.....	107
7.3.2.2. Gestione dell'informativa periodica.....	109
Premessa.....	109
Descrizione del processo.....	110
Principi di controllo.....	111
Principi di comportamento.....	113
7.3.2.3. Predisposizione dei prospetti informativi.....	115
Premessa.....	115
Descrizione del processo.....	115
Principi di controllo.....	116
Principi di comportamento.....	117
7.3.2.4. Acquisto, gestione e cessione di partecipazioni.....	119
Premessa.....	119
Descrizione del processo.....	119
Principi di controllo.....	120
Principi di comportamento.....	121
7.4 AREA SENSIBILE CONCERNENTE I REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO, I REATI DI CRIMINALITÀ ORGANIZZATA, I REATI TRANSNAZIONALI E I REATI CONTRO LA PERSONA	124
7.4.1 Fattispecie di reato.....	124
7.4.2 Attività aziendali sensibili.....	131
7.5 AREA SENSIBILE CONCERNENTE I REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ DI AUTORICICLAGGIO.	133
7.5.1 Fattispecie di reato.....	133
7.5.2 Attività aziendali sensibili.....	137
7.5.2.1. Contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose	140
Premessa.....	140

Descrizione del processo.....	140
Principi di controllo.....	141
Principi di comportamento.....	144
7.6 AREA SENSIBILE CONCERNENTE I REATI E ILLECITI AMMINISTRATIVI RICONDUCEBILI AD ABUSI DI MERCATO	148
7.6.1 <i>Fattispecie di reato</i>	148
7.6.2 <i>Attività aziendali sensibili</i>	150
7.6.2.1. Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato	152
Premessa.....	152
Descrizione del processo.....	153
Principi di controllo.....	154
Principi di comportamento.....	156
7.6.2.2 Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato.....	160
Premessa.....	160
Descrizione del processo.....	161
Principi di controllo.....	162
Principi di comportamento.....	163
7.7 AREA SENSIBILE CONCERNENTE I REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO	168
7.7.1 <i>Fattispecie di reato</i>	168
7.7.2 <i>Attività aziendali sensibili</i>	169
7.7.2.1. Gestione dei rischi in materia di salute e sicurezza sul lavoro.....	170
Premessa.....	170
Descrizione del processo.....	171
Principi di controllo.....	174
Principi di comportamento.....	177
7.8 AREA SENSIBILE CONCERNENTE I REATI INFORMATICI	179
7.8.1 <i>Fattispecie di reato</i>	179
7.8.2 <i>Attività aziendali sensibili</i>	185
7.8.2.1. Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo.....	186
Premessa.....	186
Descrizione del processo.....	187
Principi di controllo.....	188
Principi di comportamento.....	192
7.9 AREA SENSIBILE CONCERNENTE I REATI CONTRO L'INDUSTRIA E IL COMMERCIO E I REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE.....	196
7.9.1 <i>Fattispecie di reato</i>	196
7.9.2 <i>Attività aziendali sensibili</i>	202
7.10 AREA SENSIBILE CONCERNENTE I REATI AMBIENTALI	204
7.10.1 <i>Fattispecie di reato</i>	204
7.10.2 <i>Attività aziendali sensibili</i>	207
7.10.2.1 Gestione dei rischi in materia ambientale	209
Premessa.....	209
Descrizione del processo.....	209
Principi di controllo.....	210
Principi di comportamento.....	211

Capitolo 1 - Il contesto normativo

1.1 Il regime di responsabilità amministrativa previsto dal Decreto Legislativo n. 231/01 a carico delle persone giuridiche, società ed associazioni

In attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 (di seguito denominato il "Decreto" o anche "D.Lgs. n. 231/2001"), con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche. In particolare, si tratta della Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, della Convenzione firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri e della Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

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

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

La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti ivi espressamente previsti, gli Enti che abbiano tratto vantaggio dalla commissione del reato o nel cui interesse siano stati compiuti i reati - o gli illeciti amministrativi - presupposto di cui al Decreto medesimo. A carico dell'Ente sono irrogabili sanzioni pecuniarie e interdittive, nonché la

confisca, la pubblicazione della sentenza di condanna¹ e il commissariamento. Le misure interdittive, che possono comportare per l'Ente conseguenze più gravose rispetto alle sanzioni pecuniarie, consistono nella sospensione o revoca di licenze e concessioni, nel divieto di contrarre con la pubblica amministrazione, nell'interdizione dall'esercizio dell'attività, nell'esclusione o revoca di finanziamenti e contributi, nel divieto di pubblicizzare beni e servizi.

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

1.2 L'adozione dei modelli di organizzazione, gestione e controllo quali esimenti della responsabilità amministrativa dell'Ente

Istituita la responsabilità amministrativa degli Enti, l'art. 6 del Decreto stabilisce che l'Ente non risponde nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, *“modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi”*.

La medesima norma prevede, inoltre, l'istituzione di un *organismo di controllo interno all'Ente* con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza dei predetti modelli, nonché di curarne l'aggiornamento.

Il Modello di organizzazione, gestione e controllo (di seguito denominato anche “Modello”) deve rispondere alle seguenti esigenze:

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

Ove il reato venga commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia

¹ Con la Legge finanziaria approvata nel mese di luglio 2011, è stato modificato l'art. 36 del codice penale, norma espressamente richiamata dall'art. 18 del D.Lgs. n. 231/2001. La modifica stabilisce che, a seguito di condanna per la società ai sensi del D.Lgs. n. 231/2001, la pubblicazione di tale provvedimento avverrà esclusivamente sul sito internet del Ministero della Giustizia, e non anche sui quotidiani.

finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che: (i) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi; (ii) il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento è stato affidato a un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo; (iii) i soggetti hanno commesso il reato eludendo fraudolentemente il Modello; (iv) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

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

L'art. 6 del Decreto dispone, infine, che il Modello possa essere adottato sulla base di codici di comportamento redatti da associazioni rappresentative di categoria e comunicati al Ministero della Giustizia.

Si precisa che il presente Modello è stato predisposto e aggiornato attenendosi – nel rispetto delle peculiarità dell'attività della SGR e della sua struttura organizzativa – ai principi e ai contenuti del Modello della Capogruppo Intesa Sanpaolo S.p.A. e della sua Controllante FIDEURAM – Intesa Sanpaolo Private Banking S.p.A. (di seguito anche "Controllante"), nonché ispirandosi sia alle Linee Guida redatte dall'ABI sia al "Codice di Comportamento" emanato dall'Associazione italiana delle società ed enti di gestione mobiliare e immobiliare (ASSOGESTIONI). Sia le Linee Guida ABI che il Codice di Comportamento ASSOGESTIONI sono stati approvati dal Ministero della Giustizia.

Capitolo 2 - Il Modello di organizzazione, gestione e controllo di Fideuram Investimenti SGR S.p.A.

2.1 Gli strumenti aziendali esistenti quali presupposti del Modello

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

Fideuram Investimenti SGR S.p.A. (di seguito denominata anche “SGR” o “Società”), controllata da FIDEURAM – Intesa Sanpaolo Private Banking S.p.A. e appartenente al Gruppo Bancario Intesa Sanpaolo, presta:

- il servizio di gestione collettiva del risparmio;
- il servizio di gestione di portafogli;
- il servizio di consulenza in materia di investimenti.

Gli organi di Fideuram Investimenti SGR S.p.A. hanno dedicato e continuano a dedicare la massima cura nella definizione delle strutture organizzative e delle procedure operative in linea con le direttive della Capogruppo, sia al fine di assicurare efficienza, efficacia e trasparenza nella gestione delle attività e nell’attribuzione delle correlative responsabilità, sia allo scopo di ridurre al minimo disfunzioni, malfunzionamenti e irregolarità (tra i quali si annoverano anche comportamenti illeciti o comunque non in linea con quanto indicato dalla Società).

Il contesto organizzativo di Fideuram Investimenti SGR S.p.A. è costituito dall’insieme di regole, strutture e procedure che garantiscono il funzionamento della Società; si tratta dunque di un sistema articolato che viene definito e verificato internamente anche al fine di rispettare le previsioni normative a cui Fideuram Investimenti SGR S.p.A. è sottoposta sia in qualità di SGR che di società appartenente al gruppo bancario Intesa Sanpaolo (Testo Unico dell’intermediazione finanziaria e le conseguenti disposizioni emanate dalle Autorità di Vigilanza).

In tale sua qualità la SGR è sottoposta alla vigilanza di Banca d’Italia e di Consob, ognuna per i profili di rispettiva competenza, le quali svolgono verifiche e controlli sull’operato della SGR e su aspetti relativi alla sua struttura organizzativa, come previsto dalla normativa.

In quanto appartenente al gruppo bancario Intesa Sanpaolo, la SGR è inoltre sottoposta alla attività di indirizzo, governo e supporto esercitata dalla Capogruppo ed è tenuta ad osservare le disposizioni emanate dalla stessa nel quadro delle attività di governo delle proprie partecipate.

E’ dunque evidente che tale complesso di norme speciali, nonché la sottoposizione all’esercizio costante della vigilanza da parte delle Authority preposte, costituiscono anche un prezioso

strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

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

- le regole di *corporate governance* adottate in recepimento della normativa societaria e regolamentare rilevante e delle direttive emanate dalla Capogruppo;
- i regolamenti interni e le policy aziendali;
- il Codice Etico e il Codice Interno di Comportamento di Gruppo;
- il sistema dei controlli interni;
- il sistema dei poteri e delle deleghe.

Le regole, le procedure e i principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello ma fanno parte del più ampio sistema di organizzazione, gestione e controllo che lo stesso intende integrare e che tutti i soggetti destinatari, sia interni che esterni, sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la SGR.

Nei paragrafi che seguono si intendono illustrare, per grandi linee, esclusivamente i principi di riferimento del Codice Etico e del Codice Interno di Comportamento di Gruppo, il sistema dei controlli interni, nonché il sistema dei poteri e delle deleghe.

2.1.1 Codice Etico e Codice Interno di Comportamento di Gruppo

A conferma dell'importanza attribuita ai profili etici e a coerenti comportamenti improntati a rigore e integrità, la SGR recepisce il Codice Etico e il Codice Interno di Comportamento di Gruppo adottati da Intesa Sanpaolo S.p.A..

Il Codice Etico rappresenta la “carta costituzionale” del Gruppo Intesa Sanpaolo che, attraverso esso, rende espliciti i fondamenti della propria cultura aziendale e i valori di riferimento dai quali fa derivare regole concrete di comportamento verso tutti i soggetti interni ed esterni (i c.d. “stakeholder”), che hanno direttamente o indirettamente una relazione con la SGR: i clienti, gli azionisti e i collaboratori in primo luogo, ma anche i fornitori, i partner commerciali, la comunità, i territori e l'ambiente in cui il Gruppo opera.

Il Codice Interno di Comportamento di Gruppo, applicabile a tutte le Società del Gruppo, è costituito da un insieme, volutamente snello, di regole sia di carattere generale – che definiscono le norme essenziali di comportamento degli esponenti aziendali, dei dipendenti e dei collaboratori esterni che, nell'ambito delle loro funzioni, sono tenuti ad esercitare le loro attività con professionalità, diligenza, onestà e correttezza - sia di carattere più specifico, ad esempio laddove si vietano determinate operazioni personali.

2.1.2 Le caratteristiche salienti del sistema dei controlli interni

Fideuram Investimenti SGR S.p.A., per garantire una sana e prudente gestione, coniuga la profittabilità dell'impresa con un'assunzione dei rischi consapevole e con una condotta operativa improntata a criteri di correttezza.

Pertanto, la SGR, in linea con la normativa di legge e di Vigilanza e in coerenza con le indicazioni della Capogruppo e della Controllante FIDEURAM – Intesa Sanpaolo Private Banking, si è dotata di un sistema dei controlli interni idoneo a rilevare, misurare e verificare nel continuo i rischi tipici dell'attività sociale.

Il sistema dei controlli interni di Fideuram Investimenti SGR S.p.A. è insito nell'insieme di regole, procedure e strutture organizzative che mirano ad assicurare il rispetto delle strategie aziendali e il conseguimento delle seguenti finalità:

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

Il sistema dei controlli interni è delineato da un'infrastruttura documentale (impianto normativo) che permette di ripercorrere in modo organico e codificato le linee guida, le procedure, le strutture organizzative, i rischi e i controlli presenti in azienda, recependo, oltre agli indirizzi aziendali e le indicazioni degli Organi di Vigilanza, anche le disposizioni di Legge, ivi compresi i principi dettati dal D.Lgs. n. 231/2001.

L'impianto normativo è costituito da "Documenti di Governance", tempo per tempo adottati, che sovrintendono al funzionamento della SGR (Statuto, Codice Etico, Codice Interno di Comportamento di Gruppo, Regolamento di Gruppo, Regolamento delle operazioni con parti correlate, Facoltà e poteri, Policy, Linee guida, Funzionigrammi delle Strutture Organizzative, Modelli organizzativi, ecc.) e da norme più strettamente operative che regolamentano i processi aziendali, le singole attività e i relativi controlli (Comunicazioni, Procedure, Manuali, etc.).

Più nello specifico le regole aziendali disegnano soluzioni organizzative che:

- assicurano una sufficiente separatezza tra le strutture operative e quelle di controllo ed evitano situazioni di conflitto di interesse nell'assegnazione delle competenze;
- sono in grado di identificare, misurare e monitorare adeguatamente i principali rischi assunti nei diversi segmenti operativi;
- consentono la registrazione di ogni fatto di gestione e, in particolare, di ogni operazione con adeguato grado di dettaglio, assicurandone la corretta attribuzione sotto il profilo temporale;

- assicurano sistemi informativi affidabili e idonee procedure di reporting ai diversi livelli direzionali ai quali sono attribuite funzioni di controllo;
- garantiscono che le anomalie riscontrate dalle unità operative, dalla Struttura di Internal Audit o da altri addetti ai controlli siano tempestivamente portate a conoscenza di livelli appropriati dell'azienda e gestite con immediatezza.

Inoltre, le soluzioni organizzative aziendali prevedono attività di controllo a ogni livello operativo che consentano l'univoca e formalizzata individuazione delle responsabilità, in particolare nei compiti di controllo e di correzione delle irregolarità riscontrate.

La SGR, in coerenza con le indicazioni degli Organi di Vigilanza, ha individuato le seguenti quattro macro tipologie di controllo:

- **controlli di linea**, diretti ad assicurare il corretto svolgimento dell'operatività quotidiana e delle singole transazioni. Di norma tali controlli sono effettuati dalle strutture produttive (di business o di supporto) o incorporati nelle procedure informatiche, ovvero eseguiti nell'ambito delle attività di back office;
- **controlli sulla gestione dei rischi**, che hanno l'obiettivo di concorrere alla definizione delle metodologie di misurazione del rischio, di verificare il rispetto dei limiti assegnati alle varie unità operative e di controllare la coerenza dell'operatività delle singole strutture produttive con gli obiettivi di rischio rendimento assegnati. Essi sono affidati di norma a strutture diverse da quelle produttive;
- **controlli di conformità**, costituiti da politiche e procedure in grado di individuare, valutare controllare e gestire il rischio conseguente al mancato rispetto di leggi, provvedimenti delle autorità di vigilanza e norme di autoregolamentazione, nonché di qualsiasi altra norma applicabile alla SGR;
- **revisione interna**, volta a individuare andamenti anomali, violazioni delle procedure e della regolamentazione, nonché a valutare la funzionalità del complessivo sistema dei controlli interni. Essa è condotta da strutture diverse e indipendenti da quelle produttive.

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

I controlli coinvolgono, con ruoli diversi, il Consiglio di Amministrazione, il Collegio Sindacale, i Comitati istituiti dalla SGR, la Direzione Generale, la Struttura di Internal Audit, tutto il personale, e rappresentano un attributo imprescindibile dell'attività quotidiana della Società.

In particolare, l'attività di revisione interna in Fideuram Investimenti SGR S.p.A. è svolta in outsourcing dalla Struttura Audit di FIDEURAM – Intesa Sanpaolo Private Banking (di seguito "Audit"), la quale riporta direttamente al Consiglio di Amministrazione della SGR. Tale Struttura ha anche il compito di portare all'attenzione del Consiglio di Amministrazione e del Collegio Sindacale

proposte di possibili miglioramenti alle politiche di gestione dei rischi, agli strumenti di misurazione, ai processi e alle procedure.

2.1.3 Il sistema dei poteri e delle deleghe

Il Sistema dei poteri e delle deleghe trova una specifica disciplina di riferimento, fatte comunque salve le disposizioni di legge in materia, nello Statuto della SGR che prevede un'accurata ripartizione delle competenze tra gli Organi Sociali e stabilisce eventuali riserve esclusive di attribuzione.

Lo Statuto, in particolare:

- prevede che la rappresentanza legale della Società, di fronte ai terzi e in giudizio, e la firma sociale spettano al Presidente;
- investe il Consiglio di Amministrazione di tutti i poteri per la gestione ordinaria e straordinaria della Società.

Inoltre, il Consiglio ha la facoltà di compiere tutti gli atti che ritiene opportuni per il raggiungimento e l'attuazione dello scopo sociale, esclusi soltanto quelli che la legge, in modo tassativo, riserva all'Assemblea.

Il Consiglio di Amministrazione – fatte salve le competenze non delegabili a norma di legge e di statuto – ha conferito, inoltre, proprie attribuzioni all'Amministratore Delegato/Direttore Generale e ad altri soggetti determinandone i poteri e stabilendone i limiti e i meccanismi di informazione al soggetto delegante.

Il Consiglio determina gli obiettivi, le strategie e le politiche aziendali nonché le politiche di investimento dei Fondi e dei patrimoni in gestione (ivi inclusi i limiti e le procedure previsti per minimizzare i rischi delle situazioni di conflitto di interessi) con riferimento al profilo rischio/rendimento, verificandone periodicamente la corretta attuazione.

L'Amministratore Delegato/Direttore Generale ha il potere di assumere, promuovere e licenziare, nell'ambito del budget approvato dal Consiglio di Amministrazione e tenuto conto delle direttive impartite dallo stesso Consiglio di Amministrazione, il personale tutto fino al grado di dirigente escluso, stabilendone il grado, il trattamento economico ed i miglioramenti.

Il Consiglio di Amministrazione approva l'assunzione e la nomina dei dirigenti/direttori della SGR, su proposta dell'Amministratore Delegato/Direttore Generale.

Oltre a ciò, il Consiglio di Amministrazione approva la struttura organizzativa e l'attribuzione di compiti e responsabilità alle unità operative e agli addetti e altresì i processi di investimento, verificandone periodicamente l'adeguatezza.

Il Consiglio, poi, ha stabilito i poteri di spesa conferiti ai Responsabili delle strutture della SGR, in coerenza con le responsabilità gestionali attribuite, predeterminando i valori massimi di riferimento

e fissando i principi per un corretto esercizio del potere di sub-delega. La facoltà di sub-delega viene esercitata attraverso un processo trasparente, sempre monitorato, graduato in funzione del ruolo e della posizione ricoperta dal sub-delegato, prevedendo comunque l'obbligo di informativa al soggetto delegante.

Al fine di determinare le modalità di svolgimento dei diversi processi aziendali è prevista l'emanazione di specifiche procedure operative della SGR.

In relazione a quanto sopra, quindi, i principali processi decisionali e attuativi riguardanti l'operatività della SGR sono codificati, monitorabili e conoscibili da tutta la Società.

Anche i poteri di firma sociale per gli atti, i contratti, i documenti e la corrispondenza – interna ed esterna – della SGR sono formalmente predeterminati.

2.2 Le finalità perseguite con l'adozione del Modello

Nonostante gli strumenti aziendali illustrati nei paragrafi precedenti risultino di per sé idonei anche a prevenire i reati contemplati dal Decreto, la SGR, ha ritenuto opportuno adottare uno specifico Modello di organizzazione, gestione e controllo ai sensi del Decreto, nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione 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 amministrativi previsti dalla normativa di riferimento.

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

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

2.3 Gli elementi fondamentali del Modello

Il Modello di Fideuram Investimenti SGR S.p.A. è stato predisposto in coerenza con la volontà del Legislatore, tenuto conto delle linee guida emanate dalle associazioni di categoria (ABI e ASSOGESTIONI) e dei criteri e delle linee guida utilizzati da Capogruppo nella redazione del proprio Modello.

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

- individuazione delle aree di attività a rischio ovvero delle attività aziendali sensibili nel cui ambito potrebbero configurarsi le ipotesi di reato da sottoporre ad analisi e monitoraggio;
- gestione di processi operativi in grado di garantire:
 - 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;
 - una chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa;
 - corrette modalità di svolgimento delle attività medesime;
 - la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali o informatici;
 - processi decisionali legati a predefiniti criteri oggettivi (es.: esistenza di albi fornitori, esistenza di criteri oggettivi di valutazione e selezione del personale, ecc.);
 - l'esistenza e la tracciabilità delle attività di controllo e supervisione compiute sulle transazioni aziendali;
 - la presenza di meccanismi di sicurezza in grado di assicurare un'adeguata protezione/accesso fisico-logico ai dati e ai beni aziendali;
- emanazione di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale;
- definizione delle responsabilità nell'adozione, modifica, attuazione e controllo del Modello stesso;
- identificazione dell'Organismo di Vigilanza e attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- definizione dei flussi informativi nei confronti dell'Organismo di Vigilanza;
- definizione e applicazione di disposizioni idonee a sanzionare il mancato rispetto delle misure indicate nel Modello;

- formazione del personale e comunicazione interna in merito al contenuto del Decreto e del Modello e agli obblighi che ne conseguono.

2.4 La struttura del Modello

Nel definire il presente “Modello di organizzazione, gestione e controllo” Fideuram Investimenti SGR S.p.A. ha adottato un approccio che ha consentito di utilizzare e integrare nel Modello stesso le regole e la normativa interna esistenti sulla base della mappatura delle aree e attività sensibili effettuata in occasione della predisposizione del precedente Modello e dell’aggiornamento della medesima tramite il diretto coinvolgimento dei Responsabili delle Strutture della Società.

Sono state così identificate per ciascuna categoria di “illeciti presupposto”, le aree aziendali “sensibili”. Nell’ambito di ogni area sensibile sono state poi individuate le attività aziendali nello svolgimento delle quali è più verosimile il rischio della commissione di illeciti presupposto previsti dal Decreto (c.d. attività “sensibili”), codificando per ciascuna di dette attività, principi di comportamento e di controllo - diversificati in relazione allo specifico rischio-reato da prevenire - cui devono attenersi tutti coloro che vi operano.

Il Modello trova poi piena ed efficace attuazione nella realtà della SGR attraverso il collegamento di ciascuna attività “sensibile” con le strutture aziendali tempo per tempo coinvolte e con la gestione dinamica dei processi e della relativa normativa interna di riferimento, che si basa sui principi di comportamento e di controllo enunciati per ciascuna di dette attività.

L’approccio seguito:

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

In Fideuram Investimenti SGR S.p.A. il presidio dei rischi rivenienti dal n. D.Lgs. n. 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.

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

- il contesto normativo di riferimento;

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

L'impianto normativo della SGR, costituito dai "Documenti di Governance" (Statuto, Codice Etico, Codice Interno di Comportamento di Gruppo, Regolamenti, Policy, Regole, ecc.), nonché da Comunicazioni, Procedure, Manuali e altri strumenti, regola ai vari livelli l'operatività della SGR nelle aree/attività "sensibili" e costituisce a tutti gli effetti parte integrante del Modello.

L'impianto normativo è contenuto e catalogato, con specifico riferimento ad ogni attività "sensibile", in un apposito repository documentale, diffuso all'interno di tutta la SGR tramite la rete Intranet aziendale e costantemente aggiornato a cura delle strutture competenti in coerenza con l'evolversi dell'operatività.

Pertanto, dall'associazione dei contenuti del Modello con l'impianto normativo aziendale è possibile estrarre, per ciascuna delle attività "sensibili", specifici, puntuali e sempre aggiornati Protocolli che descrivono fasi di attività, strutture coinvolte, principi di controllo e di comportamento, regole operative di processo e che consentono di rendere verificabile e congrua ogni fase di attività.

2.5 I destinatari del Modello

Il Modello e le disposizioni ivi contenute e richiamate devono essere rispettate dagli esponenti aziendali e da tutto il personale di Fideuram Investimenti SGR S.p.A. e, in particolare, da parte di coloro che si trovino a svolgere le attività sensibili.

La formazione del personale e l'informazione interna sul contenuto del Modello vengono costantemente assicurati con le modalità meglio descritte al successivo Capitolo 6.

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

impegni il contraente ad attenersi ai principi del Modello e a segnalare all'Organismo di Vigilanza eventuali notizie della commissione di illeciti o della violazione del Modello.

2.6 Adozione, efficace attuazione e modificazione del Modello – Ruoli e responsabilità

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, su proposta dell'Amministratore Delegato.

L'Amministratore Delegato/Direttore Generale definisce la struttura del Modello da sottoporre all'approvazione del Consiglio di Amministrazione con il supporto, per gli ambiti di rispettiva competenza, delle strutture Compliance, Audit, Legale, Affari Societari, Antiriciclaggio, Servizi Operativi e Organizzazione e Outsourcing, Datore di Lavoro e Committente ai sensi del D.Lgs. 81/2008, e sentito il parere dell'Organismo di Vigilanza.

Efficace attuazione e modificazione del Modello

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

Il Consiglio di Amministrazione delega le singole strutture a dare attuazione ai contenuti del Modello e a curare il costante aggiornamento e implementazione della normativa interna e dei processi aziendali, che costituiscono parte integrante del Modello, nel rispetto dei principi di controllo e di comportamento definiti in relazione ad ogni attività sensibile.

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 Unità Organizzative nelle aree sensibili;
- dai responsabili delle varie Unità Organizzative della SGR in relazione alle attività a rischio dalle stesse svolte.

Il Consiglio di Amministrazione deve inoltre garantire, anche attraverso l'intervento dell'Organismo di Vigilanza, l'aggiornamento delle aree sensibili e del Modello, in relazione alle esigenze di adeguamento che si rendessero necessarie nel futuro.

Specifici ruoli e responsabilità nella gestione del Modello sono inoltre attribuiti alle Strutture di seguito indicate, alcune delle quali sono state accentrate presso FIDEURAM – Intesa Sanpaolo Private Banking.

Si rileva che nel prosieguo del presente documento saranno utilizzati indifferentemente i termini “Struttura” ovvero “Unità Organizzativa”, per indicare indistintamente le strutture previste dall’organigramma/fuzionigramma della SGR ovvero - con riguardo alle attività svolte in outsourcing - quelle della Capogruppo, della Controllante e di altre Società del Gruppo Intesa Sanpaolo.

Audit

L’Audit assicura in generale una costante e indipendente azione di sorveglianza sul regolare andamento dell’operatività e dei processi al fine di prevenire o rilevare l’insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l’efficacia e l’efficienza dei processi aziendali. Procede, pertanto, con un approccio risk based definito di concerto con la Compliance, all’effettuazione di specifiche attività di assurance volte a verificare che l’operatività posta in essere sia coerente con quanto previsto dalla normativa interna.

L’Audit supporta direttamente l’Organismo di Vigilanza nel vigilare sul rispetto e sull’adeguatezza delle regole contenute nel Modello, attivando, a fronte delle eventuali criticità riscontrate nel corso della propria attività, le strutture di volta in volta competenti per le opportune azioni di mitigazione.

Compliance

La Compliance è competente a garantire, nel tempo, la presenza di regole, procedure e prassi operative che prevengano efficacemente violazioni o infrazioni alle norme vigenti.

Con specifico riferimento ai rischi di responsabilità amministrativa introdotti dal Decreto, la Compliance supporta l’Organo di Vigilanza nello svolgimento delle sue attività di controllo mediante:

- la definizione e l’aggiornamento del Modello, con la collaborazione delle strutture Legale e Organizzazione e Outsourcing, in coerenza all’evoluzione della normativa di riferimento ed alle modifiche della struttura organizzativa aziendale, del Datore di lavoro e del Committente ai sensi del D.Lgs. n. 81/2008 e della Struttura Antiriciclaggio, per quanto di competenza;
- il monitoraggio nel tempo in merito alla efficacia del Modello con riferimento alle regole e principi di comportamento per la prevenzione dei reati sensibili; a tal fine la Compliance:
 - individua periodicamente, di concerto con Audit, i processi ritenuti a maggior grado di rischiosità in base sia a considerazioni di natura qualitativa rispetto ai reati presupposto sia all’esistenza o meno di specifici presidi a mitigazione del relativo rischio; per i

processi individuati, la Compliance provvede al rilascio di una concordanza preventiva, anteriormente alla loro pubblicazione sul sistema normativo aziendale, circa la corretta previsione nell'ambito della normativa interna dei principi di controllo e di comportamento indicati dal Modello;

- analizza le risultanze del processo di autovalutazione e attestazione delle Unità Organizzative circa il rispetto dei principi di controllo e comportamento prescritti nel Modello;
- l'esame dell'informativa proveniente dall'Audit in merito alle criticità riscontrate nel corso della propria attività di verifica.

Antiriciclaggio

La Struttura Antiriciclaggio verifica nel continuo che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione di norme di eteroregolamentazione (leggi e norme regolamentari) e di autoregolamentazione in materia di riciclaggio e di finanziamento al terrorismo.

Per il perseguimento delle finalità di cui al Decreto, la Struttura Antiriciclaggio limitatamente alla gestione dei rischi in materia di antiriciclaggio e di finanziamento del terrorismo:

- partecipa alla definizione della struttura del Modello e all'aggiornamento dello stesso;
- promuove le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio di riciclaggio e di finanziamento del terrorismo;
- riceve e inoltra i reporting periodici e i flussi informativi previsti dalle "Linee Guida per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi" e dal Modello di organizzazione, gestione e controllo adottato nel gruppo FIDEURAM – Intesa Sanpaolo Private Banking per l'antiriciclaggio e il contrasto al finanziamento del terrorismo;
- cura, in raccordo con le altre strutture competenti in materia di formazione, la predisposizione di adeguate attività formative, finalizzate a conseguire un aggiornamento su base continuativa dei dipendenti e dei collaboratori.

Legale

La Struttura Legale, per il perseguimento delle finalità di cui al Decreto, assicura assistenza e consulenza legale alle strutture della SGR, seguendo l'evolversi della normativa specifica e degli orientamenti giurisprudenziali in materia.

Spetta altresì alla Struttura Legale l'interpretazione della normativa, la risoluzione di questioni di diritto e l'identificazione delle condotte che possono configurare ipotesi di reato.

La Struttura Legale collabora con le strutture Compliance, Audit, Organizzazione e Outsourcing, Antiriciclaggio, con il Datore di lavoro e con il Committente ai sensi del D.Lgs. n. 81/2008 all'adeguamento del Modello, segnalando anche eventuali estensioni dell'ambito di responsabilità amministrativa degli Enti.

Affari Societari

Affari Societari ha la responsabilità sia di assicurare consulenza e assistenza con specifico riferimento alle caratteristiche e alle attività dell'Organismo di Vigilanza sia di segnalare ai competenti Organi societari, in caso di operazioni societarie o di altra natura che modifichino l'ambito di operatività della Società, l'esigenza di modificare il Modello per tenere conto della nuova situazione.

Servizi Operativi

Con riferimento al Decreto, Servizi Operativi, di concerto con la Struttura Personale di FIDEURAM – Intesa Sanpaolo Private Banking (di seguito “Personale”), come in dettaglio illustrato al Capitolo 5 ed al Capitolo 6:

- programma piani di formazione e interventi di sensibilizzazione rivolti a tutto il personale sull'importanza di un comportamento conforme alle regole aziendali, sulla comprensione dei contenuti del Modello, del Codice Interno di Comportamento e del Codice Etico, nonché specifici corsi destinati al personale che opera nelle aree 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 strutture Audit, Compliance, Antiriciclaggio e Legale, il processo di rilevazione e gestione delle violazioni del Modello, nonché il conseguente processo sanzionatorio 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.

Organizzazione e Outsourcing

Organizzazione e Outsourcing (di seguito “Organizzazione”), 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:

- progettare la struttura organizzativa, definendone missioni, organigrammi e funzioni, al fine di sottoporla all'approvazione dell'Amministratore Delegato;
- definire le regole per il disegno, l'ufficializzazione e la gestione dei processi organizzativi;

- supportare la progettazione dei processi organizzativi ovvero validare procedure definite da altre strutture, garantendone la coerenza con il disegno organizzativo complessivo;
- identificare, per ogni processo aziendale sensibile, l'Unità Organizzativa prevalente responsabile dell'autodiagnosi e dei flussi informativi destinati all'Organismo di Vigilanza;
- collaborare con le Unità Organizzative, con le strutture Audit, Compliance, Legale, Antiriciclaggio, con il Datore di lavoro e il Committente ai sensi del D.Lgs. n. 81/2008 e con le altre strutture aziendali interessate, ognuna per il proprio ambito di competenza, all'adeguamento del sistema normativo e del Modello (a seguito di modifiche nella normativa applicabile, nell'assetto organizzativo aziendale e/o nelle procedure operative, rilevanti ai fini del Decreto);
- diffondere la normativa interna a tutta la struttura della SGR attraverso la rete Intranet aziendale.

Unità Organizzative

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

Agli specifici fini del Decreto, le Unità Organizzative hanno la responsabilità di:

- rivedere - alla luce dei principi di comportamento e di controllo prescritti per la disciplina delle attività sensibili - le prassi ed 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 Unità Organizzative per le attività aziendali sensibili devono prestare la massima e costante cura nel verificare l'esistenza e nel porre rimedio ad 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.

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

I soggetti individuati quali Datore di Lavoro e Committente ai sensi del D.Lgs. n. 81/2008, limitatamente ai rispettivi ambiti di competenza per la gestione dei rischi in materia di sicurezza e salute sul lavoro e nei cantieri temporanei o mobili:

- partecipano alla definizione della struttura del Modello e all'aggiornamento dello stesso;
- individuano e valutano l'insorgenza di fattori di rischio dai quali possano derivare la commissioni di illeciti presupposto;

- promuovono le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio di non conformità.

2.7 Attività oggetto di outsourcing

Il modello organizzativo di Fideuram Investimenti SGR S.p.A. prevede l'esternalizzazione (di seguito anche "outsourcing") di attività aziendali, o parte di esse, presso la Capogruppo Intesa Sanpaolo S.p.A., la Controllante FIDEURAM – Intesa Sanpaolo Private Banking S.p.A. (es.: antiriciclaggio, contabilità, bilancio e fiscale, gestione delle attività di contenzioso, gestione e amministrazione del personale, segreteria societaria, attività di verifica previste dalla Direttiva sul Market Abuse, ricezione e trasmissione di ordini, etc.) e/o altre Società del Gruppo e società terze (State Street Bank GmbH - Succursale Italia, per servizi amministrativi di back office per le gestioni individuali, tenuta dell'Archivio Unico Informatico, etc.).

L'affidamento in outsourcing di tali attività è realizzato in conformità alle prescrizioni delle competenti Autorità di Vigilanza ed è formalizzato attraverso la stipula di specifici contratti che assicurano alla SGR:

- di assumere ogni decisione nel rispetto della propria autonomia, mantenendo la necessaria responsabilità su tutte le attività, ivi comprese quelle relative ai servizi esternalizzati;
- di mantenere conseguentemente i poteri di indirizzo e sulle attività esternalizzate.

In particolare, i contratti di outsourcing devono prevedere:

- una descrizione dettagliata delle attività esternalizzate;
- le modalità di erogazione dei servizi;
- gli specifici livelli di servizio;
- i poteri di verifica e controllo spettanti alla Società;
- le modalità di tariffazione dei servizi resi;
- idonei sistemi di reporting;
- adeguati presidi a tutela del patrimonio informativo della Società e della sicurezza delle transazioni;
- l'obbligo dell'outsourcer di operare in conformità alle leggi e ai regolamenti vigenti nonché di esigere l'osservanza delle leggi e dei regolamenti anche da parte di terzi ai quali si dovesse rivolgere per lo svolgimento delle attività esternalizzate;
- la facoltà per Fideuram Investimenti SGR S.p.A. di risolvere il contratto in caso di violazione da parte dell'outsourcer: (i) delle norme legislative e delle disposizioni impartite dall'Autorità di Vigilanza che possano comportare sanzioni a carico del committente; (ii) dell'obbligo di dare esecuzione all'attività nel rispetto dei principi contenuti nel Modello di Organizzazione,

Gestione e Controllo ai sensi del D.Lgs. n. 231/2001 adottato dalla SGR nonché del Codice Etico e del Codice Interno di Comportamento di Gruppo.

Apposite strutture della SGR verificano nel continuo, anche tramite il controllo dei previsti livelli di servizio, il rispetto delle clausole contrattuali e, di conseguenza, l'adeguatezza delle attività prestate dall'outsourcer.

Non sono regolate da contratti di outsourcing le attività svolte istituzionalmente dalla Capogruppo in tale sua qualità, tra cui quelle finalizzate a definire le linee strategiche del Gruppo e delle Società che lo compongono e volte a garantire l'uniformità nei processi e nelle azioni.

2.8 Il ruolo della Capogruppo e della Controllante FIDEURAM – Intesa Sanpaolo Private Banking

Ferma restando l'autonoma responsabilità di ciascuna Società appartenente al Gruppo Intesa Sanpaolo in ordine all'adozione e all'efficace attuazione di un proprio Modello ai sensi del Decreto, Intesa Sanpaolo, nell'esercizio della sua peculiare funzione di Capogruppo, ha il potere di impartire criteri e direttive di carattere generale e di verificare mediante le proprie funzioni Compliance, Internal Audit e Affari Societari e Partecipazioni, la rispondenza dei Modelli delle società appartenenti al Gruppo a tali criteri e direttive.

FIDEURAM – Intesa Sanpaolo Private Banking replica nei confronti delle proprie società controllate il medesimo approccio adottato dalla Capogruppo. La Controllante potrà quindi verificare mediante le proprie Strutture Compliance, Internal Audit e Affari Societari, la rispondenza del Modello di Fideuram Investimenti SGR S.p.A. ai criteri e alle direttive di cui sopra.

2.8.1 Principi di indirizzo di Gruppo in materia di Responsabilità amministrativa degli Enti

Allo scopo di uniformare a livello di Gruppo le modalità attraverso cui recepire e attuare i contenuti del Decreto predisponendo modalità di presidio del rischio adeguate, vengono di seguito delineati i principi di indirizzo definiti da FIDEURAM – Intesa Sanpaolo Private Banking, che ha recepito quelli della Capogruppo Intesa Sanpaolo, a cui tutte le società di diritto italiano del Gruppo, e quindi anche Fideuram Investimenti SGR S.p.A., devono attenersi, nel rispetto della propria autonomia giuridica e dei principi di corretta gestione societaria.

In particolare, la Società deve:

1. adottare il proprio Modello, dopo aver individuato le attività aziendali che presentano un rischio di commissione degli illeciti previsti dal Decreto e le misure più idonee a prevenirne la realizzazione. Nella predisposizione del Modello la Società deve attenersi ai principi e ai contenuti del Modello di Capogruppo e di FIDEURAM – Intesa Sanpaolo Private Banking salvo che sussistano situazioni specifiche relative alla natura, dimensione o al tipo di attività

esercitata nonché alla struttura societaria, all'organizzazione e/o all'articolazione delle deleghe interne che impongano o suggeriscano l'adozione di misure differenti al fine di perseguire più efficacemente gli obiettivi del Modello, nel rispetto comunque dei predetti principi nonché di quelli espressi nel Codice Etico e nel Codice Interno di Comportamento di Gruppo.

In presenza di rilevanti difformità rispetto ai principi e ai contenuti del Modello di Capogruppo e di FIDEURAM – Intesa Sanpaolo Private Banking devono essere trasmesse alla Compliance della Controllante le ragioni che le hanno motivate, nonché la bozza finale del Modello prima della sua approvazione da parte degli Organi Sociali.

L'avvenuta adozione del Modello è comunicata dalla Società alla Compliance di FIDEURAM – Intesa Sanpaolo Private Banking mediante trasmissione di copia del medesimo e della delibera di approvazione da parte del Consiglio di Amministrazione.

Resta fermo che fino a che il Modello non sia approvato, la Società adotta ogni misura idonea per la prevenzione dei comportamenti illeciti. Gli adempimenti di cui al presente punto sono di competenza della Compliance di Fideuram Investimenti SGR S.p.A.;

2. provvedere tempestivamente alla nomina dell'Organismo di Vigilanza, in linea con le indicazioni fornite dalla Capogruppo in relazione ai soggetti da nominare.

L'informativa di avvenuta nomina dell'Organismo è comunicata, mediante trasmissione di copia della delibera del Consiglio di Amministrazione, alla Compliance di FIDEURAM – Intesa Sanpaolo Private Banking. Gli adempimenti di cui al presente punto sono di competenza di Affari Societari (della Controllante);

3. assicurare il sistematico aggiornamento del Modello in funzione di modifiche normative e organizzative, nonché nel caso in cui significative e/o ripetute violazioni delle prescrizioni del Modello lo rendessero necessario. Le modifiche normative sono segnalate alla Società dalla Compliance di FIDEURAM – Intesa Sanpaolo Private Banking con apposita comunicazione. L'avvenuto aggiornamento del Modello è comunicato alla Compliance di FIDEURAM – Intesa Sanpaolo Private Banking con le modalità sopra illustrate. Gli adempimenti di cui al presente punto sono di competenza della Compliance di Fideuram Investimenti SGR S.p.A.;
4. predisporre, coordinandosi con Personale e Compliance di FIDEURAM – Intesa Sanpaolo Private Banking, attività di formazione e di comunicazione rivolte indistintamente a tutto il personale nonché interventi specifici di formazione destinati a figure impegnate in attività maggiormente sensibili al Decreto, con l'obiettivo di creare una conoscenza diffusa e una cultura aziendale adeguata in materia. Gli adempimenti di cui al presente punto sono di competenza della Compliance e di Servizi Operativi (formazione personale) di Fideuram Investimenti SGR S.p.A.;

5. adottare un idoneo presidio dei processi sensibili al Decreto che preveda la loro identificazione, documentazione e pubblicazione all'interno del sistema normativo aziendale. Inoltre, tra i processi sensibili devono essere individuati annualmente, con un approccio *risk based*, quelli ritenuti a maggior grado di rischio in base sia a considerazioni di natura qualitativa rispetto ai reati presupposto sia all'esistenza o meno di specifici presidi a mitigazione del relativo rischio. Per tali processi la Società provvede:
 - a) al rilascio di una concordanza preventiva, anteriormente alla loro pubblicazione sul sistema normativo aziendale, circa la corretta previsione nell'ambito della normativa interna dei principi di controllo e di comportamento indicati dal Modello,
 - b) all'effettuazione di specifiche attività di assurance volte a verificare che l'operatività posta in essere sia coerente con quanto previsto dalla normativa interna.Gli adempimenti di cui al punto 5-a) sono di competenza della Compliance, con il supporto di Organizzazione; gli adempimenti di cui al punto 5-b) sono di competenza dell'Audit;
6. avviare, con cadenza annuale, il processo di autodiagnosi sulle attività svolte al fine di attestare il livello di attuazione del Modello, con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative. L'attivazione del processo di autodiagnosi viene effettuato coordinandosi con Risk Management e Compliance di FIDEURAM – Intesa Sanpaolo Private Banking. Gli adempimenti di cui al presente punto sono di competenza della Compliance, di concerto - ove necessario - con Operational Risk Management di Fideuram Investimenti SGR S.p.A.;
7. fornire alla Compliance di FIDEURAM – Intesa Sanpaolo Private Banking copia delle relazioni periodiche, comprensive anche delle risultanze del processo di autodiagnosi, presentate dalla Compliance all'Organismo di Vigilanza. Gli adempimenti di cui al presente punto sono di competenza della Compliance di Fideuram Investimenti SGR S.p.A..

L'Organismo di Vigilanza della Società provvede inoltre a trasmettere all'Organismo di Vigilanza di FIDEURAM – Intesa Sanpaolo Private Banking la relazione periodica, di norma semestrale, sull'attività svolta presentata al Consiglio di Amministrazione, corredandola con le eventuali osservazioni del Consiglio stesso.

Con riferimento alle attività sopra illustrate le competenti Strutture di FIDEURAM – Intesa Sanpaolo Private Banking forniscono alla Società supporto e collaborazione, per quanto di rispettiva competenza, nell'espletamento dei compiti alle stesse spettanti.

Anche in ottemperanza al "Regolamento attuativo delle Linee guida di compliance di Gruppo" con il quale la Società ha recepito le disposizioni del "Regolamento attuativo delle Linee guida di compliance di gruppo di FIDEURAM – Intesa Sanpaolo Private Banking", la SGR, con riferimento alla responsabilità amministrativa degli Enti, è tenuta a trasmettere alla Compliance e all'Audit di

FIDEURAM – Intesa Sanpaolo Private Banking, copia dell'avviso di convocazione delle riunioni dell'Organismo di Vigilanza, dei relativi verbali e copia dell'avviso di convocazione delle riunioni degli Organi Sociali, qualora all'ordine del giorno rientrino argomenti connessi al Decreto.

Si rammenta che la competenza e la responsabilità per l'approvazione e l'efficace attuazione del Modello e per la nomina dell'Organismo di Vigilanza restano in capo alla Società, cui competono, inoltre, le seguenti attività:

- iter di formalizzazione e approvazione del Modello presso i competenti Organi sociali;
- archiviazione e conservazione della documentazione concernente i risultati dell'autodiagnosi e delle rendicontazioni predisposte agli Organi sociali.

Capitolo 3 - L'Organismo di Vigilanza

3.1 Individuazione dell'Organismo di Vigilanza

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

L'Organismo di Vigilanza deve possedere caratteristiche di autonomia, indipendenza, professionalità e continuità di azione necessarie per il corretto ed efficiente svolgimento delle funzioni ad esso assegnate. Esso inoltre deve essere dotato di poteri di iniziativa e di controllo sulle attività della Società, senza disporre di poteri gestionali e/o amministrativi.

Tenuto conto di quanto disposto dal comma 4 bis dell'art. 6 del D.Lgs. n. 231/2001, come introdotto dall'art. 14, comma 12, L. 12 novembre 2011 n. 183 ("Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato – Legge di stabilità 2012"), la Società ha ritenuto di affidare le funzioni di Organismo di Vigilanza al Collegio Sindacale.

Dell'avvenuto affidamento di tali funzioni al Collegio Sindacale è data formale comunicazione a tutti i livelli aziendali.

Il Collegio nello svolgimento di dette funzioni opera sulla base di uno specifico regolamento approvato dal medesimo e mantenendo distinte e separate le attività svolte quale Organismo di Vigilanza da quelle svolte nella sua qualità di organo di controllo della Società.

Ogni disposizione concernente l'Organismo di Vigilanza contenuta nel Modello deve intendersi riferita al Collegio Sindacale, nell'esercizio delle specifiche funzioni ad esso assegnate dal Decreto, fatto salvo quanto previsto ai successivi paragrafi 3.3.3, 3.3.4 e 3.4 nelle quali l'Organismo di Vigilanza avrà una composizione diversa rispetto a quella del Collegio Sindacale.

3.2 Composizione, funzionamento e compensi dell'Organismo di Vigilanza

Il Collegio Sindacale svolge le funzioni di Organismo di Vigilanza per tutto il periodo in cui resta in carica e nella composizione tempo per tempo determinata in applicazione delle regole di sostituzione, integrazione, sospensione e decadenza dei suoi membri proprie dell'organo, fatto salvo quanto previsto ai successivi paragrafi 3.3.3, 3.3.4 e 3.4.

Il compenso spettante per lo svolgimento delle funzioni di Organismo di Vigilanza è stabilito dall'Assemblea degli azionisti in sede di nomina del Collegio Sindacale.

L'Organismo di Vigilanza si avvale ordinariamente delle strutture della Società per l'espletamento dei suoi compiti di vigilanza e controllo ed in primis dell'Audit, struttura istituzionalmente dotata di competenze tecniche e risorse, umane e operative, idonee a garantire lo svolgimento su base continuativa delle verifiche, delle analisi e degli altri adempimenti necessari. L'Audit partecipa a tutte le riunioni dell'Organismo.

Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, l'Organismo di Vigilanza può inoltre avvalersi di consulenti esterni.

Per il presidio degli ambiti normativi specialistici l'Organismo si avvale anche delle strutture interne funzionalmente competenti e dei ruoli aziendali istituiti ai sensi delle specifiche normative di settore (Datore di lavoro, Responsabile del Servizio Prevenzione e Protezione, Rappresentante dei Lavoratori per la sicurezza, Medico competente, Responsabile della Struttura Antiriciclaggio², Referente Interno Antiriciclaggio, Responsabile delle segnalazioni di operazioni sospette, Dirigente Preposto alla redazione dei documenti contabili societari, etc.).

L'Organismo di Vigilanza, direttamente o per il tramite delle varie strutture aziendali all'uopo designate, ha accesso a tutte le attività svolte dalla Società e dagli outsourcer e alla relativa documentazione, sia presso gli uffici centrali sia presso le strutture periferiche della SGR e degli outsourcer.

Onde poter svolgere, in assoluta indipendenza, le proprie funzioni, l'Organismo di Vigilanza dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dal Consiglio di Amministrazione, su proposta dell'Organismo stesso.

3.3 Requisiti di eleggibilità, cause di decadenza e sospensione

3.3.1 Requisiti di professionalità, onorabilità ed indipendenza

Fermi restando i requisiti di professionalità, onorabilità e indipendenza disposti dalla disciplina legale e regolamentare applicabile alla Società, al fine di dotare il Collegio Sindacale di competenze

² Come definito nel Modello di organizzazione, gestione e controllo adottato nel gruppo FIDEURAM – Intesa Sanpaolo Private Banking per l'antiriciclaggio e il contrasto al finanziamento del terrorismo.

aggiuntive per il migliore svolgimento delle funzioni di Organismo di Vigilanza ad esso assegnate, almeno uno dei membri effettivi deve essere scelto tra esperti (quali, ad esempio, docenti o liberi professionisti) in materie giuridiche, economiche, finanziarie o tecnico-scientifiche ovvero tra magistrati in quiescenza o comunque tra soggetti in possesso di competenze specialistiche adeguate alla funzione derivanti, ad esempio, dall'aver svolto per un congruo periodo di tempo attività professionali in materie attinenti al settore nel quale la Società opera e/o dall'aver una adeguata conoscenza dell'organizzazione, dei sistemi dei controlli e dei principali processi aziendali ovvero dell'aver fatto – o di fare – parte di Organismi di Vigilanza.

In aggiunta al possesso dei requisiti sopra richiamati i membri effettivi ed i membri supplenti dovranno essere in possesso dei seguenti ulteriori **requisiti di onorabilità**, secondo i quali non possono essere eletti componenti dell'Organismo di Vigilanza coloro i quali:

- siano stati condannati, con sentenza irrevocabile o con sentenza non definitiva anche se a pena condizionalmente sospesa, fatti salvi gli effetti della riabilitazione, per uno dei reati tra quelli per i quali è applicabile il D.Lgs. n. 231/2001. Per sentenza di condanna si intende anche quella pronunciata ai sensi dell'art. 444 c.p.p., fatti salvi gli effetti della declaratoria giudiziale di estinzione del reato ai sensi dell'art. 445, comma secondo, c.p.p.;
- abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, anche con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- abbiano subito l'applicazione delle sanzioni amministrative accessorie previste dall'art. 187-quater del D.Lgs. n. 58/1998.

3.3.2 Verifica dei requisiti

L'Organismo di Vigilanza verifica, entro trenta giorni dalla nomina, la sussistenza, in capo ai propri componenti effettivi e supplenti, dei requisiti richiesti, sulla base di una dichiarazione resa dai singoli interessati, comunicando l'esito di tale verifica al Consiglio di Amministrazione.

L'infedele dichiarazione da parte del componente dell'Organismo ne determina l'immediata decadenza da tale funzione.

3.3.3 Cause di decadenza

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

- incorrano nella revoca o decadenza della carica di sindaco, anche in conseguenza del venir meno dei requisiti di professionalità, onorabilità e indipendenza prescritti dalla legge o dallo Statuto;

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

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

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una causa di decadenza, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione alla carica di sindaco, convoca senza indugio il Consiglio di Amministrazione affinché proceda – nella sua prima riunione successiva all'avvenuta conoscenza – alla dichiarazione di decadenza dell'interessato dalla carica di componente dell'Organismo di Vigilanza. Contestualmente - e sempre che la decadenza non dipenda dalla cessazione anche della carica di sindaco, nel qual caso opereranno le regole codicistiche di integrazione dell'organo - il Consiglio di Amministrazione provvede alla sua sostituzione con il sindaco supplente più anziano d'età.

In caso di decadenza di un sindaco supplente, in assenza di provvedimenti di sostituzione dell'Assemblea e comunque sino all'emanazione di essi, provvederà alla sostituzione il Consiglio di Amministrazione.

3.3.4 Cause di sospensione

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

- si accerti, dopo la nomina, che i componenti dell'Organismo di Vigilanza hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento non definitivo (compresa la sentenza emessa ai sensi

dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;

- i componenti dell'Organismo di Vigilanza siano stati condannati con sentenza non definitiva, anche a pena sospesa condizionalmente ai sensi dell'art. 163 c.p. (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.) per uno dei reati tra quelli per i quali è applicabile il D.Lgs. n. 231/2001;
- l'applicazione in via non definitiva delle sanzioni amministrative accessorie previste dall'art. 187 quater del D.Lgs. n. 58/1998.

In tali casi il Consiglio di Amministrazione dispone la sospensione della qualifica di membro dell'Organismo di Vigilanza e la cooptazione ad interim con il sindaco supplente più anziano di età.

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

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una delle cause di sospensione dianzi citate, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione alla carica di sindaco, convoca senza indugio il Consiglio di Amministrazione affinché provveda, nella sua prima riunione successiva, a dichiarare la sospensione del soggetto, nei cui confronti si è verificata una delle cause di cui sopra, dalla carica di componente dell'Organismo di Vigilanza. In tal caso subentra ad interim il sindaco supplente più anziano di età.

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

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

3.4 Temporaneo impedimento di un componente effettivo

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente effettivo dell'Organismo di Vigilanza di svolgere le proprie funzioni ovvero di svolgerle con la necessaria indipendenza ed autonomia di giudizio, questi è tenuto a dichiarare la sussistenza del legittimo impedimento, e, qualora esso sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva astenendosi dal partecipare alle sedute dell'Organismo stesso o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso.

A titolo esemplificativo, costituiscono cause di temporaneo impedimento:

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

Nel caso di temporaneo impedimento, subentra automaticamente e in via temporanea il sindaco supplente più anziano di età. Il membro supplente cessa dalla carica quando viene meno la causa che ha determinato il suo subentro.

Resta salva la facoltà per il Consiglio di Amministrazione, quando l'impedimento si protragga per un periodo superiore a sei mesi, prorogabile di ulteriori 6 mesi per non più di due volte, di addvenire alla revoca del componente per il quale si siano verificate le predette cause di impedimento ed alla sua sostituzione con altro componente effettivo.

3.5 Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza, nell'esecuzione della sua attività ordinaria, vigila in generale:

- sull'efficienza, efficacia ed adeguatezza del Modello nel prevenire e contrastare la commissione degli illeciti per i quali è applicabile il D.Lgs. n. 231/2001, anche di quelli che in futuro dovessero comunque comportare una responsabilità amministrativa della persona giuridica;
- sull'osservanza delle prescrizioni contenute nel Modello da parte dei destinatari, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, attraverso l'analisi dei flussi

informativi e le segnalazioni alle quali sono tenuti i responsabili delle varie strutture aziendali;

- sull'aggiornamento del Modello laddove si riscontrino esigenze di adeguamento, formulando proposte agli Organi Societari competenti, laddove si rendano opportune modifiche e/o integrazioni in conseguenza di significative violazioni delle prescrizioni del Modello stesso, di significativi mutamenti dell'assetto organizzativo e procedurale della Società, nonché delle novità legislative intervenute in materia;
- sull'esistenza ed effettività del sistema aziendale di prevenzione e protezione in materia di salute e sicurezza sui luoghi di lavoro;
- sull'attuazione delle attività formative del personale, di cui al successivo cap. 6.2;
- sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare, a seguito dell'accertata violazione del Modello.

L'Organismo di Vigilanza è inoltre chiamato a vigilare, nell'ambito delle proprie attribuzioni e competenze, sull'osservanza delle disposizioni in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo dettate dal D.Lgs. n. 231/2007 e ad effettuare le conseguenti comunicazioni interne ed esterne previste dall'art. 52 del menzionato Decreto.

Al fine di consentire all'Organismo di Vigilanza una visione d'insieme sui controlli agiti di secondo livello (conformità, antiriciclaggio, governance amministrativo-finanziaria) e di terzo livello (revisione interna), l'Audit con periodicità annuale raccoglie dalle strutture preposte i rispettivi piani delle attività di controllo pianificate sulle aree sensibili e li integra nel "Piano delle Verifiche 231".

L'Organismo di Vigilanza, sulla scorta di tale documento, valuta l'adeguatezza dei presidi delle singole attività aziendali sensibili ed indirizza eventuali ulteriori azioni di rafforzamento dei piani di controllo proposti dalle singole strutture interessate.

Le attività di controllo svolte dalle sopracitate funzioni anche per conto dell'Organismo di Vigilanza seguono appositi protocolli elaborati e costantemente aggiornati in base alle risultanze dell'analisi dei rischi e degli interventi di controllo.

L'analisi dei rischi è il processo continuo di identificazione, classificazione e valutazione preventiva dei rischi (esterni ed interni) e dei controlli interni, da cui discende il Piano delle verifiche 231.

Tale piano, predisposto annualmente, sentito anche l'Organismo di Vigilanza per quanto attiene alle materie di sua competenza, e sottoposto all'approvazione del Consiglio di Amministrazione, tiene anche conto delle eventuali osservazioni e indicazioni ricevute a vario titolo da parte degli Organi Societari.

Durante gli interventi di controllo viene analizzato nel dettaglio il livello dei controlli presenti nell'operatività e nei processi aziendali. I punti di debolezza rilevati sono sistematicamente segnalati alle Unità Organizzative e alle altre funzioni aziendali interessate al fine di rendere più efficienti ed efficaci le regole, le procedure e la struttura organizzativa. Per verificare l'effettiva esecuzione delle azioni intraprese, viene poi svolta un'attività di follow-up. Di tali attività le funzioni di controllo sopra citate rendicontano periodicamente l'Organismo di Vigilanza.

L'Organismo di Vigilanza può scambiare informazioni con la società di revisione, se ritenuto necessario o opportuno nell'ambito dell'espletamento delle rispettive competenze e responsabilità.

3.6 Modalità e periodicità di riporto agli Organi Societari

L'Organismo di Vigilanza in ogni circostanza in cui sia ritenuto necessario o opportuno, ovvero se richiesto, riferisce al Consiglio di Amministrazione circa il funzionamento del Modello e l'adempimento agli obblighi imposti dal Decreto.

L'Organismo di Vigilanza, su base almeno semestrale, trasmette al Consiglio di Amministrazione una specifica informativa sull'adeguatezza e sull'osservanza del Modello, che ha ad oggetto:

- l'attività svolta;
- le risultanze dell'attività svolta;
- gli interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione.

Dopo l'esame da parte del Consiglio di Amministrazione, l'Organismo di Vigilanza provvede ad inoltrare l'informativa - corredata delle eventuali osservazioni formulate dal Consiglio di Amministrazione - all'Organismo di Vigilanza della Controllante.

Capitolo 4 - Flussi informativi verso l'Organismo di Vigilanza

4.1 Flussi informativi da effettuarsi al verificarsi di particolari eventi

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei Dipendenti, dei Responsabili delle Strutture, degli Organi Societari, dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) in merito ad eventi che potrebbero ingenerare responsabilità di Fideuram Investimenti SGR S.p.A. ai sensi del Decreto.

Devono essere senza ritardo segnalate le:

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

Le segnalazioni possono essere effettuate dai Dipendenti, anche in forma anonima:

- direttamente all'Organismo di Vigilanza, tramite:
 - Lettera all'indirizzo "Fideuram Investimenti SGR S.p.A. – Organismo di Vigilanza, Piazza Erculea, 9 – 20122, Milano";
 - email all'indirizzo "OrganismoDiVigilanza231@fideuramSGR.it";
- per il tramite dell'Audit, al quale la segnalazione potrà essere effettuata tanto direttamente quanto mediante il Responsabile della Struttura di appartenenza, attraverso:
 - Lettera all'indirizzo "Internal Audit di Fideuram Investimenti SGR S.p.A., Piazzale Douhet, 31 - 00143, Roma";
 - email all'indirizzo "direzioneaudit@bancafideuram.it".

L'Audit, esperiti i debiti approfondimenti, informa l'Organismo di Vigilanza in merito alle segnalazioni pervenute e lo rendiconta sui fatti al riguardo riscontrati.

I soggetti esterni ivi compresi eventuali soggetti che svolgono attività in outsourcing per conto della SGR, inoltrano la segnalazione direttamente all'Organismo di Vigilanza, secondo una delle modalità sopra indicate.

L'Organismo di Vigilanza valuta le segnalazioni ricevute e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna.

L'Organismo di Vigilanza prenderà in considerazione le segnalazioni, ancorché anonime, che presentino elementi fattuali.

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

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

- per il tramite dell'Audit, le informazioni concernenti:
 - i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti ai quali è applicabile il D.Lgs. n. 231/2001, qualora tali indagini coinvolgano la SGR o suoi Dipendenti od Organi Societari o comunque la responsabilità della SGR stessa;
 - i rapporti predisposti dalle Strutture nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto;
 - i procedimenti disciplinari promossi o, nel caso in cui dette violazioni siano commesse da soggetti non dipendenti, le iniziative sanzionatorie assunte;
- per il tramite del Referente Antiriciclaggio, le segnalazioni di potenziali infrazioni di particolare gravità in materia di contrasto del riciclaggio e del finanziamento del terrorismo ai fini delle comunicazioni alle competenti Autorità ai sensi dell'art. 52 del D.Lgs. n. 231/2007.

Ciascuna Struttura aziendale a cui sia attribuito un determinato ruolo in una fase di un processo sensibile deve segnalare tempestivamente all'Organismo di Vigilanza eventuali propri comportamenti significativamente difformi da quelli descritti nel processo e le motivazioni che hanno reso necessario od opportuno tale scostamento.

L'Audit, in caso di eventi che potrebbero ingenerare gravi responsabilità di Fideuram Investimenti SGR S.p.A. ai sensi del D.Lgs. n. 231/2001, informa tempestivamente il Presidente dell'Organismo di Vigilanza e predispone specifica relazione che descriva nel dettaglio l'evento stesso, il rischio, il personale coinvolto, i provvedimenti disciplinari in corso e le soluzioni per limitare il ripetersi dell'evento.

4.2 Flussi informativi periodici

L'Organismo di Vigilanza esercita le proprie responsabilità di controllo anche mediante l'analisi di sistematici flussi informativi periodici trasmessi dalle strutture che svolgono attività di controllo di primo livello (Unità Organizzative), dall'Audit, dalla Compliance e, per quanto concerne gli ambiti normativi specialistici, dalle strutture interne funzionalmente competenti e dai ruoli aziendali istituiti

ai sensi delle specifiche normative di settore (es.: Antiriciclaggio, Datore di Lavoro, Committente, Dirigente Preposto, etc.).

Flussi informativi provenienti dalle Unità Organizzative

Con cadenza annuale i responsabili delle Unità Organizzative coinvolte nei processi “sensibili” ai sensi del D.Lgs. n. 231/2001, mediante un processo di autodiagnosi complessivo sull’attività svolta, attestano il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative.

Attraverso questa formale attività di autovalutazione, evidenziano le eventuali criticità nei processi gestiti, gli eventuali scostamenti rispetto alle indicazioni dettate dal Modello o più in generale dall’impianto normativo, l’adeguatezza della medesima regolamentazione, con l’evidenziazione delle azioni e delle iniziative adottate o al piano per la soluzione.

Le attestazioni delle Unità Organizzative sono inviate con cadenza annuale alla Compliance, la quale archiverà la documentazione, tenendola a disposizione dell’Organismo di Vigilanza per il quale produrrà una relazione con le risultanze.

La metodologia sull’esecuzione del processo di autodiagnosi, che rientra nel più generale processo di Operational Risk Management della SGR, è preventivamente sottoposta ad approvazione dell’Organismo di Vigilanza.

Flussi informativi provenienti dall’Audit

Il flusso di rendicontazione dell’Audit verso l’Organismo di Vigilanza consiste in:

- relazioni trimestrali e annuali, con le quali quest’ultimo è informato sulle verifiche svolte, sulle principali risultanze, sulle azioni di contenimento poste in essere dalle Unità interessate, sugli ulteriori interventi di controllo in programma nel trimestre successivo, in linea con il Piano Annuo di Audit;
- Piano delle Verifiche 231 annuale, derivante dall’integrazione in un unico documento dell’insieme delle attività di controllo sulle aree sensibili pianificate dalla stessa funzione e dalle funzioni Compliance, Antiriciclaggio e Governance Amministrativo-Finanziaria; detto documento è finalizzato a consentire all’Organismo di Vigilanza una visione d’insieme sui controlli agiti di secondo e di terzo livello dalle strutture incaricate dei controlli nell’ambito di ciascuna area sensibile.

Laddove ne ravvisi la necessità, l’Organismo di Vigilanza richiede all’Audit copia dei report di dettaglio per i punti specifici che ritiene di voler meglio approfondire.

Flussi informativi provenienti dalla Compliance

I flussi di rendicontazione della Compliance verso l'Organismo di Vigilanza consistono in relazioni semestrali, con le quali viene comunicato l'esito dell'attività svolta in relazione all'adeguatezza e al funzionamento del Modello, alle variazioni intervenute nei processi e nelle procedure (avvalendosi, a tal fine, della collaborazione di organizzazione) nonché agli interventi correttivi e migliorativi pianificati (inclusi quelli formativi) e al loro stato di realizzazione. L'informativa viene estesa al Consiglio di Amministrazione nell'ambito delle relazioni semestrali di compliance, che contengono uno specifico riferimento in merito alle attività svolte e ai presidi riconducibili all'ambito normativo "Responsabilità amministrativa degli Enti".

Flussi informativi provenienti dall'Antiriciclaggio

I flussi di rendicontazione periodici dell'Antiriciclaggio verso l'Organismo di Vigilanza consistono in relazioni semestrali in accordo con le "Linee Guida per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi" e con il Modello di organizzazione, gestione e controllo adottato nel gruppo FIDEURAM – Intesa Sanpaolo Private Banking per l'antiriciclaggio e il contrasto al finanziamento del terrorismo.

Flussi informativi da parte del Datore di lavoro ai sensi del D.Lgs. n. 81/2008

Il flusso di rendicontazione del Datore di lavoro ai sensi del D.Lgs. n. 81/2008 verso l'Organismo di Vigilanza è incentrato su relazioni con cadenza almeno annuale con le quali viene comunicato l'esito della attività svolta in relazione alla organizzazione e al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza.

Flussi informativi da parte del Committente ai sensi del D. Lgs. n. 81/2008

Il flusso di rendicontazione del Committente ai sensi degli artt. 88 e segg. del D.Lgs. n. 81/2008 verso l'Organismo di Vigilanza è incentrato su relazioni con cadenza almeno annuale con le quali viene comunicato l'esito della attività svolta in relazione all'organizzazione e al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza nei cantieri temporanei o mobili.

Flussi informativi da parte del Dirigente Preposto alla redazione dei documenti contabili societari ai sensi dell'art. 154-bis del D.Lgs. n. 58/98 (T.U.F.)

I flussi di rendicontazione del Dirigente Preposto alla redazione dei documenti contabili societari verso l'Organismo di Vigilanza consistono nelle relazioni periodiche previste nelle "Linee guida di governo amministrativo finanziario".

Flussi informativi provenienti da Servizi Operativi (Organizzazione e Outsourcing)

Il flusso di rendicontazione di Organizzazione e outsourcing consiste in:

- informativa con periodicità annuale concernente le principali variazioni intervenute nella struttura organizzativa, la loro rilevanza ex D.Lgs. 231/01, nonché lo stato di allineamento del sistema dei poteri (facoltà, deleghe e poteri);
- informativa con cadenza almeno annuale concernente i provvedimenti disciplinari comminati al personale dipendente nel periodo di riferimento preventivamente condivisa, prima della trasmissione all'OdV, con la Struttura Personale della Controllante.

Capitolo 5 - Il sistema sanzionatorio

Principi generali

L'efficacia del Modello è assicurata - oltre che dall'elaborazione di meccanismi di decisione e di controllo tali da eliminare o ridurre significativamente il rischio di commissione degli illeciti penali e amministrativi per i quali è applicabile il D.Lgs. n. 231/2001 - dagli strumenti sanzionatori posti a presidio dell'osservanza delle condotte prescritte.

I comportamenti del personale di Fideuram Investimenti SGR S.p.A. e dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) non conformi ai principi e alle regole di condotta prescritti nel presente Modello - ivi ricomprendendo il Codice Etico, il Codice Interno di Comportamento di Gruppo e le procedure e norme interne, che fanno parte integrante del Modello - costituiscono illecito contrattuale.

Su tale presupposto, la SGR adotterà nei confronti:

- del personale dipendente assunto con contratto regolato dal diritto italiano e dai contratti collettivi nazionali di settore, il sistema sanzionatorio stabilito dal Codice disciplinare della SGR e dalle leggi e norme contrattuali di riferimento;
- di tutti i soggetti esterni il sistema sanzionatorio stabilito dalle disposizioni contrattuali e di legge che regolano la materia.

L'attivazione, sulla base delle segnalazioni pervenute dall'Audit o dall'Organismo di Vigilanza, lo svolgimento e la definizione del procedimento disciplinare nei confronti dei dipendenti sono affidati, nell'ambito delle competenze alla stessa attribuite, al Responsabile Servizi Operativi con il supporto della Struttura Personale della Controllante.

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

Gli interventi sanzionatori nei confronti di eventuali dipendenti distaccati da altre Società del Gruppo sono affidati alla competente funzione Risorse Umane della Società di appartenenza.

Il tipo e l'entità di ciascuna delle sanzioni stabilite, saranno applicate, ai sensi della normativa richiamata, tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di eventuale recidiva, nonché dell'attività lavorativa svolta dall'interessato e della relativa posizione funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.

Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento e definizione dell'eventuale azione penale, in quanto i principi e le regole di condotta imposte dal Modello sono

assunte dalla SGR in piena autonomia e indipendentemente dai possibili reati che eventuali condotte possano determinare e che l'autorità giudiziaria ha il compito di accertare.

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

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di Vigilanza, il quale riceve dai Servizi Operativi un'informativa con cadenza almeno annuale sui provvedimenti disciplinari comminati al personale dipendente nel periodo di riferimento.

Personale appartenente alle aree professionali e ai quadri direttivi

1) il provvedimento del **rimprovero verbale** si applica in caso:

di lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello, correlandosi detto comportamento ad una *“lieve inosservanza delle norme contrattuali o delle direttive e istruzioni impartite dalla direzione o dai superiori”* ai sensi di quanto già previsto al **punto a)** del Codice disciplinare vigente;

2) il provvedimento del **rimprovero scritto** si applica in caso:

di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da poter essere considerata ancorché non lieve, comunque, non grave, correlandosi detto comportamento ad una *“inosservanza non grave delle norme contrattuali o delle direttive e istruzioni impartite dalla direzione o dai superiori”* ai sensi di quanto previsto al **punto b)** del Codice disciplinare vigente;

3) il provvedimento della **sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni** si applica in caso:

di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva, correlandosi detto comportamento ad una *“inosservanza - ripetuta o di una certa gravità - delle norme contrattuali o delle direttive e istruzioni impartite dalla direzione o dai superiori”* ai sensi di quanto previsto al **punto c)** del Codice disciplinare vigente;

4) il provvedimento del **licenziamento per giustificato motivo** si applica in caso:

di adozione, nell'espletamento delle attività comprese nelle aree sensibili, di un comportamento caratterizzato da notevole inadempimento delle prescrizioni e/o delle procedure e/o delle norme interne stabilite dal presente Modello, anche se sia solo suscettibile di configurare uno degli illeciti per i quali è applicabile il Decreto, correlandosi detto comportamento ad una *“violazione (...) tale da configurare (...) un inadempimento “notevole” degli obblighi relativi”* ai sensi di quanto previsto al **punto d)** del Codice disciplinare vigente;

5) il provvedimento del **licenziamento per giusta causa** si applica in caso:

di adozione, nell'espletamento delle attività comprese nelle aree sensibili, di un comportamento consapevole in contrasto con le prescrizioni e/o le procedure e/o le norme interne del presente Modello, che, ancorché sia solo suscettibile di configurare uno degli illeciti a cui per i quali è applicabile il Decreto, leda l'elemento fiduciario che caratterizza il rapporto di lavoro ovvero risulti talmente grave da non consentirne la prosecuzione, neanche provvisoria, correlandosi detto comportamento ad una *“mancanza di gravità tale (o per dolo del fatto, o per i riflessi penali o pecuniari o per la recidività o per la sua particolare natura) da far venir meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire la prosecuzione del rapporto stesso”* ai sensi di quanto previsto alla **lettera e)** del Codice disciplinare vigente.

Personale dirigente

In caso di violazione, da parte di dirigenti, dei principi, delle regole e delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività comprese nelle aree sensibili di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili i provvedimenti di seguito indicati, tenuto altresì conto della gravità della/e violazione/i e della eventuale reiterazione. Anche in considerazione del particolare vincolo fiduciario che caratterizza il rapporto tra la Società e il lavoratore con la qualifica di dirigente, sempre in conformità a quanto previsto dalle vigenti disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti delle imprese creditizie, finanziarie e strumentali si procederà con il **licenziamento con preavviso** e il **licenziamento per giusta causa** che, comunque, andranno applicati nei casi di massima gravità della violazione commessa.

Considerato che detti provvedimenti comportano la risoluzione del rapporto di lavoro, la Società, in attuazione del principio legale della gradualità della sanzione, si riserva la facoltà, per le infrazioni meno gravi di applicare la misura del **rimprovero scritto** - in caso di semplice inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello - ovvero l'altra della **sospensione dal servizio e dal trattamento economico fino ad un massimo di 10**

giorni - in caso - di inadempimento colposo di una certa rilevanza (anche se dipendente da recidiva) ovvero di condotta colposa inadempiente ai principi e alle regole di comportamento previsti dal presente Modello.

Soggetti esterni

Ogni comportamento posto in essere da soggetti esterni alla Società che, in contrasto con il presente Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata del rapporto contrattuale, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti alla SGR, come nel caso di applicazione da parte dell'Autorità Giudiziaria delle sanzioni previste dal Decreto.

Componenti del Consiglio di Amministrazione

In caso di violazione del Modello da parte di soggetti che ricoprono la funzione di componenti del Consiglio di Amministrazione di Fideuram Investimenti SGR S.p.A., l'Organismo di Vigilanza informerà il Collegio Sindacale, il quale provvederà ad adottare le iniziative ritenute opportune in relazione alla fattispecie, nel rispetto della normativa vigente.

Capitolo 6 - Formazione e comunicazione interna

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

Al riguardo è fondamentale un'attività di comunicazione e di formazione finalizzata a favorire la diffusione di quanto stabilito dal Decreto e dal Modello adottato nelle sue diverse componenti (gli strumenti aziendali presupposto del Modello, le finalità del medesimo, la sua struttura e i suoi elementi fondamentali, il sistema dei poteri e delle deleghe, l'individuazione dell'Organismo di Vigilanza, i flussi informativi verso quest'ultimo, etc.). Ciò affinché la conoscenza della materia e il rispetto delle regole che dalla stessa discendono costituiscano parte integrante della cultura professionale di ciascun collaboratore.

Con questa consapevolezza, le attività di formazione e comunicazione interna – rivolte a tutto il Personale – hanno il costante obiettivo, anche in funzione degli specifici ruoli assegnati, di creare una conoscenza diffusa e una cultura aziendale adeguata alle tematiche in questione, mitigando così il rischio della commissione di illeciti.

6.1 Comunicazione interna

I neo assunti ricevono, all'atto dell'assunzione, unitamente alla prevista restante documentazione, copia del Modello, del Codice Etico e del Codice Interno di Comportamento di Gruppo. La sottoscrizione di un'apposita dichiarazione attesta la consegna dei documenti, l'integrale conoscenza dei medesimi e l'impegno ad osservare le relative prescrizioni.

Sull'Intranet aziendale, sono pubblicate e rese disponibili per la consultazione, oltre alle varie comunicazioni interne, il Modello di Organizzazione, Gestione e Controllo della SGR e le normative collegate (in particolare, Codice Etico e Codice Interno di Comportamento di Gruppo).

I documenti pubblicati sono costantemente aggiornati in relazione alle modifiche che via via intervengono nell'ambito della normativa di legge e del Modello, i cui periodici aggiornamenti sono comunicati dal vertice aziendale a tutto il personale dipendente.

Delle novità intervenute in materia, delle attività sensibili nonché degli interventi formativi, il personale verrà informato sia tramite apposite comunicazione sull'intranet aziendale sia, ove possibile, mediante lo strumento della Web TV.

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

6.2 Formazione

Le attività formative hanno l'obiettivo di far conoscere il Decreto, il nuovo Modello e, in particolare, di sostenere adeguatamente coloro che sono coinvolti nelle attività "sensibili".

Per garantirne l'efficacia esse sono erogate tenendo conto delle molteplici variabili presenti nel contesto di riferimento; in particolare:

- i target (i destinatari degli interventi, il loro livello e ruolo organizzativo);
- i contenuti (gli argomenti attinenti al ruolo delle persone);
- gli strumenti di erogazione (aula, e-learning, Web Tv);
- i tempi di erogazione e di realizzazione (la preparazione e la durata degli interventi);
- l'impegno richiesto al target (i tempi di fruizione);
- le azioni necessarie per il corretto sostegno dell'intervento (promozione, supporto dei Capi).

Le attività prevedono:

- una formazione di base e-learning per tutto il personale;
- specifici interventi di aula per le persone che lavorano nelle strutture in cui maggiore è il rischio di comportamenti illeciti.

Il corso e-learning di base consente a ciascun partecipante di verificare le proprie conoscenze iniziali sulla materia e approfondire i soli temi sui quali non si è dimostrato adeguatamente preparato, oltre a quelli legati alle più recenti novità legislative. Il corso, per risultare completato ed essere accreditato a curriculum, prevede anche il superamento di un test finale di valutazione dell'apprendimento.

La formazione d'aula, che interviene dopo la fruizione del prodotto e-learning, declinata per specifico ambito operativo, ha l'obiettivo di diffondere la conoscenza dei reati, delle fattispecie configurabili, dei presidi specifici relativi alle aree di competenza degli operatori, e di richiamare alla corretta applicazione del Modello di Organizzazione, Gestione e Controllo. La metodologia didattica è fortemente interattiva e si avvale di *case studies*.

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

La fruizione delle varie iniziative di formazione è obbligatoria per tutto il personale cui le iniziative stesse sono dirette ed è monitorata a cura della Struttura Servizi Operativi, di concerto, ove previsto, con la Struttura Personale della Controllante, con la collaborazione dei Responsabili ai vari livelli che devono farsi garanti, in particolare, della fruizione delle iniziative di formazione "a distanza" da parte dei loro collaboratori.

La Struttura Servizi Operativi, di concerto, ove previsto, con la Struttura Personale di FIDEURAM – Intesa Sanpaolo Private Banking, ha cura di raccogliere i dati relativi alla partecipazione ai vari programmi e di archivarli, rendendoli disponibili alle funzioni interessate.

L'Organismo di Vigilanza verifica, anche attraverso i flussi informativi provenienti dalla Compliance, lo stato di attuazione delle attività formative e ha facoltà di chiedere controlli periodici sul livello di conoscenza, da parte del personale, del Decreto, del Modello e delle sue implicazioni operative.

Capitolo 7 – Gli illeciti presupposto - Aree, attività e relativi principi di comportamento e di controllo

7.1 Individuazione delle aree sensibili

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

Sono state pertanto analizzate, come illustrato al paragrafo 2.4, le fattispecie di illeciti presupposto per le quali si applica il Decreto; con riferimento a ciascuna categoria dei medesimi sono state identificate nella SGR le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

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

Il Modello trova poi piena attuazione nella realtà dell'azienda attraverso il collegamento di ciascuna area e attività “sensibile” con le strutture aziendali coinvolte e con la gestione dinamica dei processi e della relativa normativa di riferimento.

Sulla base delle disposizioni di legge attualmente in vigore le aree sensibili identificate dal Modello riguardano in via generale:

- Area Sensibile concernente i reati contro la Pubblica Amministrazione;
- Area Sensibile concernente i reati societari;
- Area Sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona;
- Area Sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- Area Sensibile concernente i reati e illeciti amministrativi riconducibili ad abusi di mercato;
- Area Sensibile concernente i reati in tema di salute e sicurezza sul lavoro;
- Area Sensibile concernente i reati informatici;
- Area Sensibile concernente i reati contro l'industria e il commercio e i reati in materia di violazione del diritto d'autore;
- Area Sensibile concernente i reati ambientali.

7.2 Area sensibile concernente i reati contro la Pubblica Amministrazione

7.2.1 Fattispecie di reato

Premessa

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

La legge 6 novembre 2012, n. 190 (cosiddetta "legge anticorruzione"), entrata in vigore il 28 novembre 2012, ha riformato la disciplina dei delitti in questione, inasprendo le pene, modificando alcune fattispecie e creandone di nuove. Conseguentemente, ha inserito nell'art. 25 del Decreto il riferimento al reato di "*Induzione indebita a dare o promettere utilità*", la cui condotta in precedenza era ricompresa nel reato di "*Concussione*". Ha inoltre introdotto il reato societario di "*Corruzione tra privati*", descritto nel Capitolo 7.3.

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

A titolo meramente esemplificativo e avendo riguardo all'operatività della Società si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione: i) lo Stato, le Regioni, le Province, i Comuni; ii) i Ministeri, i Dipartimenti, le Commissioni; iii) gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT).

Tra le fattispecie penali qui considerate, i reati di concussione e di induzione indebita a dare o promettere utilità nonché i reati di corruzione, nelle loro varie tipologie, presuppongono il coinvolgimento necessario di un soggetto privato e di un pubblico agente, vale a dire di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" e/o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p..

In sintesi, può dirsi che la distinzione tra le due figure è in molti casi controversa e labile e che la stessa è definita dalle predette norme secondo criteri basati sulla funzione oggettivamente svolta dai soggetti in questione.

La qualifica di Pubblico Ufficiale è attribuita a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. L'esercizio di una pubblica funzione amministrativa

solitamente è riconosciuto sussistere in capo a coloro che formano o concorrono a formare la volontà dell'Ente pubblico o comunque lo rappresentano di fronte ai terzi, nonché a coloro che sono muniti di poteri autoritativi o certificativi³.

A titolo meramente esemplificativo si possono menzionare i seguenti soggetti, nei quali la giurisprudenza ha individuato la qualifica di Pubblico Ufficiale: ufficiale giudiziario, consulente tecnico del giudice, curatore fallimentare, esattore o dirigente di aziende municipalizzate anche se in forma di S.p.A., assistente universitario, portalettere, funzionario degli uffici periferici dell'ACI, consigliere comunale, geometra tecnico comunale, insegnanti delle scuole pubbliche, ufficiale sanitario, notaio, dipendente dell'INPS, medico convenzionato con l'ASL, tabaccaio che riscuote le tasse automobilistiche.

La qualifica di Incaricato di Pubblico Servizio si determina per via di esclusione, spettando a coloro che svolgono quelle attività di interesse pubblico, non consistenti in semplici mansioni d'ordine o meramente materiali, disciplinate nelle stesse forme della pubblica funzione, ma alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale.

A titolo esemplificativo si elencano i seguenti soggetti nei quali la giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, lettori dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza, dipendenti del Poligrafico dello Stato, guardie giurate che conducono furgoni portavalori.

Va considerato che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un Ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato.

Deve porsi particolare attenzione al fatto che, ai sensi dell'art. 322-bis c.p., la condotta del soggetto privato – sia esso corruttore o indotto a dare o promettere utilità – è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o

³ Rientra nel concetto di poteri autoritativi non solo il potere di coercizione ma ogni attività discrezionale svolta nei confronti di soggetti che si trovano su un piano *non paritetico* rispetto all'autorità (cfr. Cass., Sez. Un. 11/07/1992, n.181). I poteri certificativi comprendono tutte quelle attività di documentazione cui l'ordinamento assegna efficacia probatoria, quale che ne sia il grado.

Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il soggetto privato persegua un indebito vantaggio per sé o per altri con riferimento ad un'operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

Si illustrano sinteticamente qui di seguito le fattispecie delittuose previste dagli artt. 24 e 25 del Decreto.

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

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

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

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

Truffa (art. 640, comma 2, n. 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui si ottenga un ingiusto profitto ponendo in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato oppure ad altro Ente Pubblico.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni da parte dello Stato, di altro Ente pubblico o delle Comunità Europee.

Gli elementi caratterizzanti il reato in esame sono: rispetto al reato di truffa generica (art. 640, comma 2, n. 1, c.p.), l'oggetto materiale specifico, che per la presente fattispecie consiste nell'ottenimento di erogazioni pubbliche comunque denominate; rispetto al reato di indebita

percezione di erogazioni (art. 316-ter c.p.), la necessità dell'ulteriore elemento della attivazione di artifici o raggiri idonei ad indurre in errore l'Ente erogante.

Frode informatica (art. 640-ter)

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

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

Concussione (art. 317 c.p.)

Parte attiva del reato di concussione può essere il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio che, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o a promettere a lui o a un terzo denaro o altre utilità non dovutegli.

La costrizione si attua mediante violenza o minaccia di un danno ingiusto (ad es.: rifiuto di compiere un atto dovuto se non contro compenso), con modalità tali da non lasciare libertà di scelta alla persona che la subisce, la quale è considerata vittima del reato e quindi esente da pena.

Pertanto, la responsabilità degli enti a titolo di concussione è configurabile, sempre che sussista l'interesse o vantaggio dell'ente, nel caso di reato commesso da un soggetto apicale o da un subordinato attraverso una condotta estorsiva posta in essere in concorso con un Pubblico Ufficiale o un Incaricato di Pubblico Servizio nei confronti di un terzo.

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

Il reato punisce la condotta dell'Incaricato di Pubblico Servizio o del Pubblico Ufficiale che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere a lui o a un terzo denaro o altre utilità non dovutegli.

Si tratta di fattispecie diversa da quella di concussione: le pressioni e richieste del pubblico agente non sono tali da esercitare la violenza morale tipica dell'estorsione, ma assumono forme di mero condizionamento della volontà della controparte, quali prospettazioni di possibili conseguenze sfavorevoli o difficoltà, ostruzionismi, ecc.. E' punita anche la condotta della persona che cede

all'induzione, corrispondendo o promettendo l'indebita utilità per evitare un danno o conseguire un vantaggio illecito.

Pertanto, la responsabilità degli enti a titolo di induzione indebita è configurabile, sempre che sussista l'interesse o vantaggio dell'ente, nel caso di reato commesso da un soggetto apicale o da un subordinato secondo una delle seguenti forme alternative:

- condotta induttiva posta in essere in concorso con un Pubblico Ufficiale o con un Incaricato di Pubblico Servizio nei confronti di un terzo;
- accettazione delle condotte induttive provenienti da un agente pubblico.

Corruzione

L'elemento comune a tutte le varie fattispecie del reato di corruzione consiste nell'accordo fra un pubblico agente (Pubblico Ufficiale o Incaricato di Pubblico Servizio) e un soggetto privato.

L'accordo corruttivo presuppone che le parti agiscano in posizione paritaria fra di loro e non ha rilevanza il fatto che l'iniziativa provenga dall'una o dall'altra parte, diversamente da quanto avviene nei reati di concussione e di induzione indebita a dare o promettere utilità, che invece richiedono che il soggetto rivestente la qualifica pubblica, paventando l'abuso dei propri poteri, faccia valere la propria posizione di superiorità, alla quale corrisponde nel privato una situazione di soggezione. Peraltro, può risultare difficile distinguere nella pratica quando ricorra una fattispecie di corruzione piuttosto che un reato di induzione indebita; la distinzione rileva innanzitutto per la determinazione della pena con la quale è punito il soggetto privato, che è più lieve nel reato di induzione indebita.

Nel fatto della corruzione si ravvisano due distinti reati: l'uno commesso dal soggetto corrotto, rivestente la qualifica pubblica (c.d. corruzione passiva), l'altro commesso dal corruttore (c.d. corruzione attiva) che, in forza della disposizione di cui all'art. 321 c.p., è punito con le stesse pene previste per il corrotto..

Le fattispecie di corruzione previste dall'art. 25 del Decreto sono le seguenti.

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

Tale ipotesi di reato si configura nel caso in cui un Pubblico Ufficiale o un Incaricato di Pubblico Servizio riceva, per sé o per o per un terzo, denaro o altra utilità, o ne accetti la promessa, per l'esercizio delle sue funzioni o dei suoi poteri. L'attività del pubblico agente può estrinsecarsi in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), ma il reato sussiste anche se l'utilità indebita è:

- corrisposta o promessa a prescindere dall'individuazione della "compravendita" di un atto ben determinato, in quanto è sufficiente il solo fatto che sia posta in relazione col generico esercizio della funzione;
- corrisposta dopo il compimento di un atto d'ufficio, anche se precedentemente non promessa.

Rilevano quindi ipotesi di pericolo di asservimento della funzione ampie e sfumate e dazioni finalizzate a una generica aspettativa di trattamento favorevole⁴.

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

Il reato, detto anche di "corruzione propria", consiste in un accordo per la promessa o dazione di un indebito compenso riferito ad un atto, da compiersi o già compiuto, contrario ai doveri del pubblico agente (ad esempio: corresponsione di denaro per garantire l'aggiudicazione di una gara).

Corruzione in atti giudiziari (art. 319-ter, comma 1, c.p.)

In questa fattispecie di reato la condotta del corrotto e del corruttore è caratterizzata dal fine specifico di favorire o di danneggiare una parte in un processo penale, civile o amministrativo.

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

Tale reato è commesso dal soggetto privato la cui offerta o promessa di denaro o di altra utilità per l'esercizio di funzioni pubbliche (art. 318 c.p.) o di un atto contrario ai doveri d'ufficio (art. 319 c.p.) non sia accettata. Per il medesimo titolo di reato risponde il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio che solleciti, con esito negativo, tale offerta o promessa.

7.2.2. Attività aziendali sensibili

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

⁴ L'art. 318 c.p. previgente alla "legge anticorruzione" contemplava la sola ipotesi della cosiddetta "corruzione impropria", vale a dire l'indebito compenso per il compimento di uno specifico atto, dovuto o comunque conforme ai doveri d'ufficio, del pubblico agente. Il comma 2 prevedeva la condotta di "corruzione impropria susseguente", vale a dire l'indebito compenso non pattuito, ma corrisposto dopo il compimento di un atto d'ufficio, ipotesi in cui era punito il corrotto, ma non il corruttore. A seguito dell'abolizione di tale comma, anche la condotta predetta rientra nella formulazione del comma 1, con la conseguenza che ora sono puniti entrambi anche in tale caso (cfr. l'art. 321 c. p.). Infine, non ha più rilevanza la qualità di dipendente pubblico dell'incaricato di pubblico servizio, che era richiesta per la sussistenza del reato in questione.

- Stipula dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo;
- Gestione dei contenziosi e degli accordi transattivi;
- Gestione dei rapporti con le Autorità di Vigilanza;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del processo di selezione e assunzione del personale.

Con riferimento all'attività sensibile concernente la Gestione e l'utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo si rimanda al relativo protocollo; si riportano qui di seguito, i protocolli che dettano i principi di controllo e i principi di comportamento applicabili alle altre sopraelencate attività sensibili e che si completano con la normativa aziendale di dettaglio che regola le attività medesime.

Detti protocolli si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.2.2.1. **Stipula dei rapporti contrattuali con la Pubblica Amministrazione**

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte in qualsiasi tipologia di stipula di rapporti contrattuali con gli Enti della Pubblica Amministrazione, aventi ad oggetto operazioni quali, a titolo esemplificativo e non esaustivo:

- stipula di contratti con Enti Pubblici aventi ad oggetto la gestione di portafogli e la sottoscrizione di quote di fondi;
- concessione di agevolazioni commissionali.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di “corruzione”, nelle loro varie tipologie, di “induzione indebita”⁵ e di “truffa ai danni dello Stato”.

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio delle attività svolte dal Collocatore nell’ambito della relativa “Convenzione di commercializzazione”.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di stipula dei rapporti contrattuali con la Pubblica Amministrazione si articola, in generale, nelle seguenti fasi:

⁵ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell’ambito degli altri Stati membri dell’Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest’ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un’attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l’emanazione di un provvedimento che ne pregiudichi l’attività economica).

- contatto con Clienti Istituzionali Pubblici;
- invio dell'informativa ai Clienti Istituzionali Pubblici;
- raccolta di informazioni, documenti e valutazione dell'opportunità di dar seguito alla proposta;
- comunicazione dell'esito della valutazione, con indicazione della tipologia di documentazione da acquisire;
- acquisizione della documentazione e valutazione degli aspetti contrattuali;
- formulazione della proposta e sottoscrizione della modulistica necessaria all'accensione del rapporto;
- accensione del rapporto.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
 - i soggetti che esercitano poteri autorizzativi e/o negoziali nei confronti della Pubblica Amministrazione sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento;
 - le fasi concernenti la formulazione della proposta commerciale e la conclusione del contratto sono precedute da un'attività di verifica, anch'essa documentata, della correttezza formale e sostanziale delle operazioni proposte (in relazione alle specifiche esigenze ed eventuali limiti agli investimenti) e della sussistenza dei poteri autorizzativi in capo al Funzionario pubblico preposto alla conclusione del contratto relativo all'operazione proposta;
 - gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto da soggetti appositamente incaricati;
 - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

- Segregazione dei compiti tra i soggetti coinvolti nel processo di definizione dell'accordo contrattuale con gli Enti pubblici. In particolare:
 - le attività di sviluppo commerciale sono svolte da strutture diverse rispetto a quelle che gestiscono operativamente l'erogazione dei prodotti/servizi contrattualizzati;
 - la definizione dell'accordo è esclusivamente affidata al Responsabile della Struttura aziendale competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati; l'atto formale della stipula del contratto avviene in base al vigente sistema dei poteri e delle deleghe;
 - i soggetti deputati alla predisposizione della documentazione per la presentazione dell'offerta tecnica ed economica, ovvero per la partecipazione a bandi di gara pubblica, sono differenti da coloro che sottoscrivono la stessa.

- Attività di controllo:
 - la documentazione relativa alla stipula dei rapporti contrattuali viene sottoposta per il controllo al Responsabile della Struttura aziendale competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati che si avvalgono, per la definizione delle nuove tipologie contrattuali, del contributo consulenziale della competente Struttura per quanto concerne gli aspetti di natura legale;
 - la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna Struttura interessata nello svolgimento delle attività inerenti l'esecuzione dei processi oggetto del presente protocollo; in particolare, dovrà essere assicurata la verifica della sussistenza di idonei poteri in capo ai soggetti facoltizzati all'effettuazione delle operazioni di investimento.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - ciascuna fase rilevante degli accordi con la Pubblica Amministrazione deve risultare da apposita documentazione scritta;
 - ogni accordo/convenzione/contratto con Enti pubblici è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nelle attività di stipula dei rapporti contrattuali con la Pubblica Amministrazione, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo. In particolare:

- tutti i soggetti che, in fase di sviluppo commerciale e identificazione di nuove opportunità di business, intrattengono rapporti con la Pubblica Amministrazione per conto della SGR, devono essere individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento;
- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della SGR, quali i contratti per la vendita di prodotti e servizi, devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1;
- qualora sia previsto il coinvolgimento di soggetti terzi nella stipula dei rapporti contrattuali con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- le procedure aziendali definiscono i criteri e le casistiche in cui il coinvolgimento di soggetti terzi deve essere preventivamente sottoposto al vaglio di una funzione indipendente;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore in ordine alla scelta di attribuzione di incarichi alla SGR o alle caratteristiche dei prodotti/servizi;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di stipulare accordi/convenzioni/contratti con la SGR;
- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della SGR. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti e affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per i soggetti predetti (es.: applicazioni di condizioni non in linea con i parametri di mercato);
- promettere versare/offrire somme di denaro non dovute, doni o gratuite prestazioni, vantaggi di qualsiasi natura, come descritti al punto precedente, a favore di esponenti apicali o di persone a loro subordinate appartenenti a società/enti partecipanti a gare pubbliche al fine di dissuaderli dalla partecipazione o per conoscere le loro offerte e formulare le proprie in modo tale da ottenere l'aggiudicazione della gara, oppure minacciarli di un danno ingiusto per le medesime motivazioni;
- affidare incarichi a consulenti esterni eludendo criteri documentabili e obiettivi, quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione, nelle loro varie tipologie, e di "induzione indebita" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare l'instaurazione/sviluppo di rapporti finalizzati alla stipula.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.2. Gestione dei rapporti contrattuali con la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione di rapporti contrattuali con gli Enti della Pubblica Amministrazione, aventi ad oggetto operazioni quali, a titolo esemplificativo e non esaustivo:

- la gestione di contratti con Enti Pubblici aventi ad oggetto la gestione di portafogli e la sottoscrizione di quote di fondi;
- concessione di agevolazioni commissionali.

Ai sensi del D.Lgs. n. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione dei reati di “corruzione”, nelle loro varie tipologie, di “induzione indebita”⁶, e “truffa ai danni dello Stato”.

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio delle attività svolte dal Collocatore nell’ambito della relativa “Convenzione di commercializzazione”.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Descrizione del processo

Il processo gestione dei rapporti contrattuali con clienti istituzionali pubblici, si articola, in generale, nelle seguenti fasi:

⁶ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell’ambito degli altri Stati membri dell’Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest’ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un’attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l’emanazione di un provvedimento che ne pregiudichi l’attività economica).

- versamento iniziale da parte del Cliente Istituzionale Pubblico;
- gestione delle operazioni successive disposte dai Clienti Istituzionali Pubblici, quali: operazioni di investimento/disinvestimento, versamenti, disposizione di bonifici, pagamento assegni, e qualsiasi operazione ordinaria disposta successivamente all'apertura del rapporto;
- presentazione ed esame della richiesta di estinzione del rapporto;
- estinzione del rapporto.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
 - la gestione dei rapporti con i Funzionari pubblici in costanza di esecuzione degli obblighi di natura contrattuale con gli Enti stessi è organizzativamente demandata a specifiche strutture della SGR che si occupano della erogazione di prodotti / servizi oggetto del contratto. La stipula dei contratti per l'esecuzione di servizi nei confronti della Pubblica Amministrazione è effettuata nel rispetto dei principi di comportamento sanciti dal Protocollo per la *"Stipula dei rapporti contrattuali con la Pubblica Amministrazione"* e, in particolare, tutti gli atti che impegnano contrattualmente la SGR nei confronti di terzi devono essere sottoscritti soltanto da soggetti appositamente incaricati;
 - nell'ambito di ogni Struttura, i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione dei rapporti contrattuali con la Pubblica Amministrazione sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento;
 - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di gestione degli accordi contrattuali con gli Enti pubblici. In particolare:

- i soggetti deputati alla predisposizione della documentazione per la rendicontazione agli enti sono differenti da coloro che sottoscrivono la stessa;
- le Strutture incaricate della gestione operativa dei prodotti/servizi contrattualizzati, sono diverse da quelle incaricate dello sviluppo commerciale.
- **Attività di controllo:** la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna Struttura interessata nello svolgimento delle attività di natura contabile/amministrativa inerenti all'esecuzione dei processi oggetto del presente protocollo. In particolare dovrà essere assicurata la verifica della regolarità delle operazioni nonché della completezza, della correttezza e della tempestività delle scritture contabili che devono essere costantemente supportate da meccanismi di maker e checker.
- **Tracciabilità del processo** sia a livello di sistema informativo sia in termini documentali:
 - la realizzazione delle operazioni nella esecuzione degli adempimenti contrattuali verso la Pubblica Amministrazione prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate. Le strutture provvedono alla archiviazione della documentazione cartacea inerente all'esecuzione degli adempimenti svolti;
 - ciascuna Struttura di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rapporti con la Pubblica Amministrazione.
- **Sistemi premianti o di incentivazione:** i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione derivanti da adempimenti di natura contrattuale con gli Enti stessi, sono tenute ad osservare le modalità espresse nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della SGR devono essere appositamente incaricati; il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/esecuzione dei rapporti contrattuali con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- in occasione di incassi effettuati agli sportelli di imposte, tasse e contributi a vario titolo, le operazioni dovranno essere svolte secondo le procedure stabilite internamente.

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore in ordine alla scelta di attribuzione di incarichi alla SGR o alle caratteristiche dei prodotti/servizi;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la SGR;
- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della SGR. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo

esemplificativo, la promessa di assunzione per parenti e affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per il pubblico ufficiale (es. applicazioni di condizioni non in linea con i parametri di mercato);

- ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite dalla SGR o, comunque, un trattamento più favorevole di quello dovuto;
- affidare incarichi a consulenti esterni eludendo criteri documentabili e obiettivi, quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione, nelle loro varie tipologie, e di "induzione indebita" che potrebbero derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la SGR.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.3. Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione quali, a titolo esemplificativo e non esaustivo:

- gestione dei rapporti con gli Enti assistenziali e previdenziali e realizzazione, nei tempi e nei modi previsti, degli adempimenti di legge in materia di lavoro e previdenza (INPS, INAIL, INPDAP, Direzione Provinciale del Lavoro, Medicina del Lavoro, Agenzia delle Entrate, Enti pubblici locali, ecc);
- gestione dei rapporti con le Camere di Commercio per l'esecuzione delle attività inerenti al registro delle imprese;
- gestione dei rapporti con gli Enti Locali territorialmente competenti in materia di smaltimento rifiuti;
- gestione dei rapporti con Amministrazioni Statali, Regionali, Comunali o Enti Locali (A.S.L., Vigili del Fuoco, Arpa, etc.) per l'esecuzione di adempimenti in materia di igiene e sicurezza e/o di autorizzazioni, permessi, concessioni;
- gestione dei rapporti con il Ministero dell'Economia e delle Finanze, con le Agenzie Fiscali e con gli Enti pubblici locali per l'esecuzione di adempimenti in materia di imposte;
- gestione dei rapporti con Banca d'Italia per l'esecuzione degli adempimenti in materia di mantenimento della riserva obbligatoria;
- gestione dei rapporti con la Prefettura, la Procura della Repubblica e le Camere di Commercio competenti per la richiesta di certificati e autorizzazioni.

Ai sensi del D.Lgs. n. 231/2001, le predette attività potrebbero presentare occasioni per la commissione dei reati di "corruzione", nelle loro varie tipologie, di "induzione indebita"⁷ e di "truffa ai danni dello Stato".

⁷ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione dei rapporti con la Pubblica Amministrazione in occasione di richieste di autorizzazioni o esecuzione di adempimenti si articola nelle seguenti fasi:

- predisposizione della documentazione;
- invio della documentazione richiesta e archiviazione della pratica;
- gestione dei rapporti con gli Enti pubblici;
- assistenza in occasione di sopralluoghi e accertamenti da parte degli Enti;
- gestione dei rapporti con gli Enti pubblici per il ritiro dell'autorizzazione e l'esecuzione degli adempimenti.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
 - nell'ambito di ogni Struttura, i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione delle attività inerenti alla richiesta di autorizzazioni alla Pubblica Amministrazione sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento;

ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

nel caso in cui i rapporti con gli Enti pubblici vengano intrattenuti da soggetti terzi, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali;

- la gestione dei rapporti con i Funzionari pubblici in caso di accertamenti/sopralluoghi, effettuati anche allo scopo di verificare l'ottemperanza alle disposizioni di legge che regolamentano l'operatività dell'area di propria competenza, è attribuita al Responsabile della Struttura di riferimento e/o ai soggetti da quest'ultimo appositamente individuati.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di gestione delle attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti verso la Pubblica Amministrazione al fine di garantire, per tutte le fasi del processo un meccanismo di maker e checker.
- Attività di controllo: le attività devono essere svolte in modo tale da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti, prevedendo, ove opportuno, specifici controlli in contraddittorio. In particolare, laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della predisposizione dei documenti richiesti dall'Ente pubblico, è effettuato un controllo sulla correttezza delle elaborazioni da parte di soggetti diversi da quelli deputati alla esecuzione delle attività.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - copia della documentazione consegnata all'Ente pubblico per la richiesta di autorizzazione o per l'esecuzione di adempimenti è conservata presso l'archivio della Struttura di competenza;
 - il Responsabile della Struttura, ovvero il soggetto aziendale all'uopo incaricato ha l'obbligo di firmare per accettazione il verbale redatto dai Funzionari pubblici in occasione degli accertamenti/sopralluoghi condotti presso la SGR, di inviarne una copia all'Audit e di mantenerne una nei propri uffici, unitamente ai relativi allegati;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla richiesta di autorizzazioni alla Pubblica Amministrazione.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione in occasione di richiesta di autorizzazioni o esecuzione di adempimenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della SGR devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalare al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1;
- qualora sia previsto il coinvolgimento di soggetti terzi (professionisti, ditte, ecc.) nell'espletamento delle attività inerenti alla richiesta di autorizzazioni ovvero nell'esecuzione di adempimenti verso la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente il riscontro da parte della Pubblica Amministrazione;

- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni al di fuori delle prassi dei regali di cortesia di modico valore e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della SGR. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti e affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per i soggetti predetti (es.: applicazioni di condizioni non in linea con i parametri di mercato);
- affidare incarichi a consulenti esterni eludendo criteri documentabili e obiettivi, quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione, nelle loro varie tipologie, e di "induzione indebita" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto con la SGR.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.2.4. Gestione dei contenziosi e degli accordi transattivi

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione dei contenziosi giudiziari e stragiudiziali (amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi con Enti pubblici o con soggetti privati.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di “corruzione”, nelle loro varie tipologie⁸, di “induzione indebita”⁹ e “truffa ai danni dello Stato” nonché del reato di “induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria”¹⁰.

Sussiste altresì il rischio della commissione del reato di “corruzione tra privati”, introdotto dalla L. n. 190/2012 tra i reati societari e descritto nel Capitolo 7.4.

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

⁸ Ivi compresa la “corruzione in atti giudiziari” (art. 319-ter comma 1, c.p.).

⁹ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell’ambito degli altri Stati membri dell’Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest’ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un’attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l’emanazione di un provvedimento che ne pregiudichi l’attività economica).

¹⁰ Tale reato, punito dall’art. 377-bis c.p., costituisce reato presupposto della responsabilità degli enti ai sensi dell’art. 25-decies del Decreto. Inoltre, ai sensi dell’art. 10 della L. n. 146/2006 può dar luogo alla medesima responsabilità anche se commesso in forma transnazionale. Si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

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

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione del contenzioso si articola nelle seguenti fasi, effettuate sotto la responsabilità delle Strutture competenti per materia, in coordinamento con la Struttura interessata dalla controversia e con gli eventuali professionisti esterni incaricati:

- apertura del contenzioso giudiziale o stragiudiziale;
 - raccolta delle informazioni e della documentazione relative alla vertenza;
 - analisi, valutazione e produzione degli elementi probatori;
 - predisposizione degli scritti difensivi e successive integrazioni, direttamente o in collaborazione con i professionisti esterni;
- gestione della vertenza;
- ricezione, analisi e valutazione degli atti relativi alla vertenza;
- predisposizione dei fascicoli documentali;
- partecipazione, ove utile o necessario, alla causa, in caso di contenzioso giudiziale;
- intrattenimento dei rapporti costanti con gli eventuali professionisti incaricati, individuati nell'ambito dell'apposito albo;
- assunzione delle delibere per:
 - determinazione degli stanziamenti al Fondo Rischi e Oneri in relazione alle vertenze passive e segnalazione dell'evento quale rischio operativo;
 - esborsi e transazioni;
- chiusura della vertenza.

Il processo di gestione degli accordi transattivi riguarda tutte le attività necessarie per prevenire o dirimere una controversia attraverso accordi o reciproche rinunce e concessioni, al fine di evitare l'instaurarsi o il proseguire di procedimenti giudiziari.

Il processo si articola nelle seguenti fasi:

- analisi dell'evento da cui deriva la controversia e verifica dell'esistenza di presupposti per addivenire alla transazione;
- gestione delle trattative finalizzate alla definizione e alla formalizzazione della transazione;
- redazione, stipula ed esecuzione dell'accordo transattivo.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti: la gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione, prevede l'accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio delle singole fasi del processo in capo a diverse Strutture, a seconda che si tratti di profili giuridici di natura amministrativa, civile, penale, fiscale, giuslavoristica e previdenziale. E' inoltre previsto, nell'ambito di ciascuna fase operativa caratteristica del processo, quanto segue:
 - il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia per la gestione del contenzioso, ivi incluso quello nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
 - il conferimento degli incarichi a legali esterni diversi da quelli individuati nell'ambito dell'albo predisposto e approvato dalla Struttura competente è autorizzato dal Responsabile della Struttura medesima o da un suo delegato.

- Segregazione dei compiti: attraverso il chiaro e formalizzato conferimento di compiti e responsabilità nell'esercizio delle facoltà assegnate nello svolgimento delle attività di cui alla gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione. In particolare, le procedure aziendali prevedono adeguati livelli quantitativi oltre ai quali le singole transazioni devono essere autorizzate da funzioni diverse da quelle di business che hanno gestito la relazione.

- Attività di controllo:
 - rilevazione e monitoraggio periodico delle vertenze pendenti;
 - verifica periodica della regolarità, della completezza e correttezza di tutti gli adempimenti connessi a vertenze / transazioni che devono essere supportati da meccanismi di maker e checker.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - ciascuna fase rilevante del processo deve risultare da apposita documentazione scritta;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è altresì responsabile dell'archiviazione e della conservazione della documentazione di competenza, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna, nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla SGR devono essere appositamente incaricati;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi, i contratti / lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalare al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo è vietato, al fine di favorire indebitamente interessi della SGR, ed anche a mezzo di professionisti esterni o soggetti terzi:

- in sede di contatti formali od informali, o nel corso di tutte le fasi del procedimento:
 - avanzare indebite richieste o esercitare pressioni su Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio);
 - indurre chiunque al superamento di vincoli o criticità ai fini della tutela degli interessi della SGR;
 - indurre - con violenza o minaccia o, alternativamente, con offerta o promessa di denaro o di altra utilità - a tacere o a mentire la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
 - influenzare indebitamente le decisioni dell'Organo giudicante o le posizioni della Pubblica Amministrazione, quando questa sia controparte del contenzioso/arbitrato;
- in occasione di ispezioni/controlli/verifiche influenzare il giudizio, il parere, il rapporto o il referto degli Organismi pubblici o nominati dall'Organo giudicante o della Polizia Giudiziaria;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute, al fine di influenzare impropriamente la gestione del rapporto con la SGR;
- promettere versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), o accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la SGR, al fine di favorire indebitamente gli interessi della SGR, oppure minacciarli di un danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per i soggetti predetti (es.: applicazione condizioni non in linea con i parametri di mercato);
- affidare incarichi a professionisti esterni eludendo criteri documentabili e obiettivi, quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del professionista devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo; ciò al fine di prevenire il rischio di commissione del

reato di corruzione, nelle loro varie tipologie, e di “induzione indebita” che potrebbe derivare dall’eventuale scelta di soggetti “vicini” a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare il rapporto con la SGR.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l’efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.5. Gestione dei rapporti con le Autorità di Vigilanza

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione dei rapporti con le Autorità di Vigilanza e riguarda qualsiasi tipologia di attività posta in essere in occasione di segnalazioni, adempimenti, comunicazioni, richieste e visite ispettive.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di “corruzione”, nelle loro varie tipologie, di “induzione indebita”¹¹ e di “ostacolo all’esercizio delle funzioni delle Autorità Pubbliche di Vigilanza” (art. 2638 del codice civile).

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti con le Autorità di Vigilanza, tra le quali, a titolo esemplificativo:

- Banca d’Italia;
- Consob;
- IVASS;
- Autorità Nazionale Anticorruzione;
- Autorità Garante per la Privacy;
- Autorità Garante per la Concorrenza e il Mercato (AGCM);

¹¹ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell’ambito degli altri Stati membri dell’Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest’ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un’attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l’emanazione di un provvedimento che ne pregiudichi l’attività economica).

- COVIP.

I principi di comportamento contenuti nel presente protocollo si applicano, a livello d'indirizzo comportamentale, anche nei confronti delle Autorità di Vigilanza estere.

Descrizione del processo

Le attività inerenti la gestione dei rapporti con le Autorità di Vigilanza sono riconducibili alle seguenti tipologie:

- elaborazione/trasmissione delle segnalazioni occasionali o periodiche alle Autorità di Vigilanza;
- richieste/istanze di abilitazioni e/o autorizzazioni;
- riscontri e adempimenti connessi a richieste/istanze delle Autorità di Vigilanza;
- gestione dei rapporti con i Funzionari delle Autorità di Vigilanza in occasione di visite ispettive.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
 - ad eccezione delle visite ispettive i rapporti con le Autorità di Vigilanza sono intrattenuti dal Responsabile della Struttura di riferimento o da soggetti dallo stesso appositamente incaricati;
 - gli atti che impegnano contrattualmente la SGR devono essere sottoscritti soltanto da soggetti incaricati.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con le Autorità di Vigilanza. In particolare:
 - con riferimento alla gestione dei rapporti non riconducibili alla ordinaria operatività delle Strutture, tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività aziendale indirizzata alle Autorità di Vigilanza è preventivamente condivisa con le competenti Strutture Legale, Audit e Affari Societari;

- è compito del Responsabile della Struttura interessata dalla visita ispettiva, dopo aver accertato l'oggetto dell'ispezione, individuare le risorse deputate a gestire i rapporti con i Funzionari pubblici durante la loro permanenza presso la SGR. Le competenti strutture Legale, Audit, Compliance e, nei casi particolarmente rilevanti, l'Organismo di Vigilanza devono essere tempestivamente informate della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall'Autorità.
- Attività di controllo:
 - controlli di completezza, correttezza e accuratezza delle informazioni trasmesse alle Autorità di Vigilanza da parte della Struttura interessata per le attività di competenza che devono essere supportate da meccanismi di maker e checker;
 - controlli di carattere giuridico sulla conformità alla normativa di riferimento della segnalazione/comunicazione richiesta;
 - controlli automatici di sistema, con riferimento alle segnalazioni periodiche.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - è fatto obbligo a tutte le Strutture della SGR, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni e adempimenti alle Autorità di Vigilanza, di archiviare e conservare la documentazione di competenza prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico. Tale documentazione deve essere resa disponibile a richiesta alle Strutture Legale, Audit e Affari Societari;
 - ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della SGR è documentata/registrata in via informatica e archiviata presso la Struttura di competenza;
 - fatte salve le situazioni in cui non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il personale della Struttura interessata che ha presenziato alla visita ispettiva assiste il Funzionario pubblico nella stesura del verbale di accertamento ed eventuale prescrizione, riservandosi le eventuali controdeduzioni, firmando, per presa visione il verbale, comprensivo degli allegati, prodotto dal Funzionario stesso;
 - ad ogni visita ispettiva da parte di Funzionari rappresentanti delle Autorità di Vigilanza il Responsabile della Struttura interessata provvede a trasmettere alle Strutture competenti copia del verbale rilasciato dal Funzionario pubblico e degli annessi allegati. Qualora non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il Responsabile della Struttura interessata dall'ispezione od un suo delegato

provvede alla redazione di una nota di sintesi dell'accertamento effettuato e alla trasmissione della stessa alle Strutture competenti. La suddetta documentazione è archiviata dal Responsabile della Struttura interessata dall'ispezione.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nel processo di gestione dei rapporti con le Autorità di Vigilanza, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della SGR devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un soggetto dell'Autorità di Vigilanza di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1;
- devono essere puntualmente trasmesse le segnalazioni periodiche alle Autorità di Vigilanza e tempestivamente riscontrate le richieste/istanze pervenute dalle stesse Autorità;
- nell'ambito delle ispezioni effettuate da parte dei Funzionari delle Autorità presso la sede della SGR, fatte salve le situazioni in cui i Funzionari richiedano colloqui diretti con personale della SGR specificamente individuato, partecipano agli incontri con i Funzionari stessi almeno due soggetti, se appartenenti alla Struttura interessata dall'ispezione; diversamente, laddove l'ispezione sia seguita da Strutture diverse da quella coinvolta dalla verifica (quali, ad esempio: Personale, Organizzazione, Legale e Audit), è prevista la partecipazione di un unico soggetto agli incontri con i Funzionari.

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

- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità di Vigilanza in errore;

- chiedere o indurre i rappresentanti dell’Autorità di Vigilanza a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l’esercizio delle funzioni di Vigilanza;
- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sè o per altri – a rappresentanti dell’Autorità di Vigilanza a titolo personale con la finalità di promuovere o favorire interessi della SGR. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti e affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per i soggetti predetti (es.: applicazioni di condizioni non in linea con i parametri di mercato).

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l’efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.6. Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione delle procedure acquisitive dei beni e dei servizi.

Tra i beni vanno considerate anche le opere dell'ingegno di carattere creativo¹², mentre tra le prestazioni vanno ricomprese anche quelle a contenuto intellettuale di qualsiasi natura (es. legale, fiscale, tecnica, giuslavoristica, amministrativa, organizzativa, incarichi di mediazione, d'agenzia o di intermediazioni varie, ecc.), ivi incluso il conferimento di incarichi professionali ovvero di consulenze.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "corruzione" nelle loro varie tipologie, e di "induzione indebita"¹³.

Sussiste altresì il rischio della commissione del reato di "corruzione tra privati", introdotto dalla L. n. 190/2012 tra i reati societari e descritto nel Capitolo 7.4.

Una gestione non trasparente del processo, infatti, potrebbe consentire la commissione di tali reati, ad esempio attraverso la creazione di fondi "neri" a seguito del pagamento di prezzi superiori all'effettivo valore del bene/servizio ottenuto.

Si intende inoltre prevenire il rischio di acquisire beni o servizi di provenienza illecita, e in particolare il coinvolgimento nei reati contro l'industria e il commercio e nei reati in materia di

¹² Ai sensi dell'art. 2575 del codice civile, le opere dell'ingegno di carattere creativo tutelate dal diritto d'autore sono quelle che appartengono alle scienze, alla letteratura (anche scientifica o didattica), alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì considerate e protette come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore (art. 1, L. 22 aprile 1941, n. 633).

¹³ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest'ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un'attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l'emanazione di un provvedimento che ne pregiudichi l'attività economica).

violazione del diritto d'autore¹⁴ e di commissione del reato di "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

L'attività di gestione delle procedure acquisitive dei beni e dei servizi si articola nei seguenti processi:

- definizione e gestione del budget;
- gestione degli approvvigionamenti;
- gestione del ciclo passivo;
- gestione dei fornitori.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti:
 - il budget della SGR è predisposto e approvato dal Consiglio di Amministrazione;
 - l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che

¹⁴ Si veda al riguardo l'"Area sensibile concernente i reati contro l'industria e il commercio e i reati in materia di violazione del diritto d'autore".

- stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
- la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa interna, fatte salve esigenze/forniture occasionali. Tali soggetti devono garantire e su richiesta poter documentare, anche con riferimento ai subappaltatori da loro incaricati:
 - in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi - il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti;
 - in relazione ai lavoratori impiegati, il rispetto della disciplina in tema di immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale;
 - l'eventuale affidamento a terzi - da parte dei fornitori della SGR - di attività in subappalto, ove non previsto all'interno del contratto stipulato con il fornitore, è subordinato ad un preventivo assenso da parte della Struttura della SGR che ha stipulato il contratto;
 - l'autorizzazione al pagamento della fattura spetta ai Responsabili delle Strutture per le quali è prevista l'assegnazione di un budget e delle relative facoltà di spesa o ai soggetti all'uopo incaricati; può essere negata a seguito di formale contestazione delle inadempienze/carenze della fornitura adeguatamente documentata e dettagliata a cura delle predette Strutture;
 - il pagamento delle fatture è effettuato da una specifica Struttura aziendale dedicata.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive. In particolare:
 - le attività di cui alle diverse fasi del processo devono essere svolte da soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
 - Attività di controllo: la normativa interna di riferimento identifica i controlli che devono essere svolti a cura di ciascuna Struttura interessata in ogni singola fase del processo:
 - verifica dei limiti di spesa e della pertinenza della stessa;
 - verifica della regolarità, completezza, correttezza e tempestività delle scritture contabili;
 - verifica del rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti, ivi compreso il controllo a campione del rispetto delle sopra

menzionate garanzie circa l'autenticità e la legittima provenienza dei beni forniti e la regolarità dei lavoratori da loro impiegati;

- verifica del rispetto delle norme di legge che vietano o subordinano a determinate condizioni il conferimento di incarichi di qualunque tipologia a dipendenti pubblici o ex dipendenti pubblici.

Per quanto concerne infine il conferimento di incarichi professionali e consulenze il cui svolgimento comporta un rapporto diretto con la Pubblica Amministrazione (quali, ad esempio, spese legali per contenzioso, onorari a professionisti per pratiche edilizie, spese per consulenze propedeutiche all'acquisizione di contributi pubblici, ecc.) i Responsabili delle Strutture interessate dovranno:

- disporre che venga regolarmente tenuto in evidenza l'elenco dei professionisti/consulenti, l'oggetto dell'incarico e il relativo corrispettivo;
 - verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
 - documentabilità di ogni attività del processo, con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista anche attraverso gare, in termini di motivazione della scelta, nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nel processo di gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali, sono tenute ad osservare le modalità esposte nel

presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- la documentazione contrattuale che regola il conferimento di incarichi di fornitura/incarichi professionali deve contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- assegnare incarichi di fornitura e incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della SGR che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi;
- minacciare i fornitori di ritorsioni qualora effettuino prestazioni a favore o utilizzino i servizi di concorrenti della SGR;
- promettere versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), o accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la SGR, al fine di favorire indebitamente gli interessi della SGR, oppure minacciarli di un

danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per i soggetti predetti (es.: applicazione di condizioni non in linea con i parametri di mercato);

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.7. Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni.

Si precisa che, ai fini del presente protocollo, valgono le seguenti definizioni:

- per “omaggi” si intendono le elargizioni di beni di modico valore offerte, nell’ambito delle ordinarie relazioni di affari, al fine di promuovere l’immagine della SGR;
- per “spese di rappresentanza” si intendono le spese sostenute dalla SGR nell’espletamento delle relazioni commerciali, destinate a promuovere e migliorare l’immagine della SGR (ad es.: spese per colazioni e rinfreschi, spese per forme di accoglienza e ospitalità, ecc.);
- per “iniziative di beneficenza” si intendono le elargizioni in denaro che la SGR destina esclusivamente ad Enti senza fini di lucro;
- per “sponsorizzazioni” si intendono la promozione, la valorizzazione e il potenziamento dell’immagine della SGR attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: società o gruppi sportivi che svolgono attività anche dilettantistica, Enti senza fini di lucro, Enti territoriali e organismi locali, ecc.).

Ai sensi del D.Lgs. n. 231/2001, i relativi processi potrebbero costituire una delle modalità strumentali attraverso cui commettere i reati di “corruzione”, nelle loro varie tipologie, e di “induzione indebita”¹⁵.

Sussiste altresì il rischio della commissione del reato di “corruzione tra privati”, introdotto dalla L. n. 190/2012 tra i reati societari e descritto nel Capitolo 7.4.

Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad

¹⁵ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell’ambito degli altri Stati membri dell’Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest’ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un’attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l’emanazione di un provvedimento che ne pregiudichi l’attività economica).

esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali e/o a persone loro subordinate di società controparti o in relazione con la SGR al fine di favorire interessi della SGR ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

I processi di gestione degli omaggi e delle spese di rappresentanza hanno ad oggetto i beni destinati ad essere offerti, in qualità di cortesia commerciale, a soggetti terzi, quali, ad esempio, clienti, fornitori, Enti della Pubblica Amministrazione, istituzioni pubbliche o altre organizzazioni.

Tali beni sono acquisiti sulla base delle regole operative sancite dalla normativa interna in materia di spesa e dal protocollo *“Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali”*.

I processi di gestione delle spese per beneficenze e per sponsorizzazioni si articolano nelle seguenti fasi:

- ricezione della richiesta, inviata dagli Enti, di elargizioni e di beneficenze o sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di *due diligence*¹⁶ della SGR;
- esame/valutazione dell'iniziativa/progetto proposto;
- autorizzazione alla spesa e, qualora previsto, stipula dell'accordo/ contratto;
- erogazione delle elargizioni da parte della SGR.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti che costituisce parte integrante e sostanziale del presente protocollo.

¹⁶ Ricerca di informazioni rilevanti sull'Ente richiedente quali, a titolo esemplificativo e non esaustivo denominazione, natura giuridica e data di costituzione, sede legale e operativa (se diversa da quella legale) ed eventuale sito web, legale rappresentante ed eventuali notizie sulla sua reputazione, notizie sull'Ente e sulle sue linee strategiche, sulla dimensione (numero dipendenti e/o collaboratori, numero di soci), sui principali progetti realizzati negli ultimi due anni nel settore di riferimento dell'iniziativa proposta, sintesi delle informazioni finanziarie relative ai bilanci approvati negli ultimi due anni, ecc.

Principi di controllo

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

- Livelli autorizzativi definiti:
 - per quanto attiene ai beni destinati ad omaggi e alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
 - tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
 - sono definiti diversi profili di utenza per l'accesso a procedure informatiche, ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
 - per quanto attiene gli omaggi e le spese di rappresentanza destinati, seppure in modo non esclusivo, ad esponenti della Pubblica Amministrazione, le procedure aziendali stabiliscono idonei limiti quantitativi rapportati al valore di tali omaggi/spese.

- Segregazione dei compiti: tra i differenti soggetti coinvolti nei processi. In particolare:
 - le attività di cui alle diverse fasi dei processi devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.

- Attività di controllo:
 - la normativa interna definisce i limiti oltre ai quali le erogazioni per beneficenze e sponsorizzazioni devono essere precedute da un'attività di *due diligence* da parte della Struttura interessata, avente ad oggetto:
 - analisi e verifica del tipo di organizzazione e della finalità per la quale è costituita;
 - verifica ed approvazione di tutte le erogazioni da parte del Responsabile della Struttura interessata;
 - che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito budget deliberato dagli Organi competenti (all'interno del quale è fissato

un limite massimo di importo e di numero di erogazioni annuali per destinatario, salvo espresse deroghe formalizzate ai livelli competenti);

- o per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa.

Inoltre i Responsabili delle Strutture interessate dovranno:

- o disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti nonché le relative date/occasioni di elargizioni. Tale obbligo non si applica per gli omaggi cosiddetti "marchiati", riportanti cioè il logotipo della SGR (quali biro, oggetti per scrivania, ecc.), nonché l'omaggistica standard predisposta dalle Strutture Centrali (ad esempio, in occasione di fine anno);
 - o verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - o completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutte le Strutture interessate, di una reportistica sulle erogazioni effettuate/contratti stipulati;
 - o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni.

Principi di comportamento

Premesso che le spese per omaggi sono consentite purché di modico valore e, comunque, tali da non compromettere l'integrità e la reputazione di una delle parti e da non influenzare l'autonomia di giudizio del beneficiario, le Strutture, a qualsiasi titolo coinvolte nella gestione di omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo. In particolare:

- la SGR può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che non contrastano con i principi etici della SGR;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le “sponsorizzazioni” non possono essere oggetto contemporaneo di erogazione per beneficenza.

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

- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di Enti coinvolti in note vicende giudiziarie, pratiche non rispettose dei diritti umani, o contrarie alle norme in tema di vivisezione e di tutela dell’ambiente..Non possono inoltre essere oggetto di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, club (ad esempio Lions, Rotary, ecc.), associazioni e gruppi ricreativi, scuole private, parificate e/o legalmente riconosciute, salvo specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico;
- effettuare elargizioni/omaggi a favore di Enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persona ad essa collegate contravvenendo a quanto previsto nel presente protocollo;
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della SGR, anche a seguito di illecite pressioni;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalare al proprio Responsabile, il quale a sua volta ha l’obbligo di trasmettere la segnalazione ricevuta all’Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell’Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1;
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti

apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la SGR, al fine di favorire indebitamente gli interessi della SGR;

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

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.2.8. Gestione del processo di selezione e assunzione del personale

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione del processo di selezione e assunzione del personale.

Il processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di “corruzione”, nelle loro varie tipologie, di “induzione indebita”¹⁷ e di “corruzione tra privati”, introdotto dalla L. n. 190/12 tra i reati societari (descritto nel Capitolo 7.4.).

Una gestione non trasparente del processo di selezione e assunzione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la promessa di assunzione verso rappresentanti della Pubblica Amministrazione, e/o esponenti apicali, e/o persone loro subordinate di società controparti o in relazione con la SGR o soggetti da questi indicati, concessa al fine di influenzarne l’indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per la SGR.

Sussiste altresì il rischio della commissione del reato di “Impiego di cittadini di paesi terzi il cui soggiorno è irregolare”.

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

¹⁷ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica amministrazione italiana, ma è pure considerata illecita e allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee, o, infine, nell’ambito degli altri Stati membri dell’Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali, purché, in quest’ultimo caso, il corruttore o il soggetto indotto persegua un indebito vantaggio per sé o per altri con riferimento ad una operazione economica internazionale ovvero agisca al fine di ottenere o di mantenere un’attività economica o finanziaria (ad esempio, al fine di evitare la risoluzione di un appalto o l’emanazione di un provvedimento che ne pregiudichi l’attività economica).

Descrizione del processo

Il processo di selezione e assunzione si articola nelle seguenti fasi:

- Selezione del personale:
 - analisi e richiesta di nuove assunzioni;
 - definizione del profilo del candidato;
 - reclutamento dei candidati;
 - effettuazione del processo selettivo;
 - individuazione dei candidati.
- Formalizzazione dell'assunzione.

Resta nelle competenze delle Strutture aziendali specificatamente facoltizzate l'istruttoria relativa alla selezione e assunzione di personale specialistico altamente qualificato ovvero di figure destinate a posizioni di vertice (cosiddetta "assunzione a chiamata").

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti:
 - la Struttura competente riceve le richieste formali di nuovo personale da parte delle Strutture interessate e le valuta in coerenza con il budget e i piani interni di sviluppo;
 - autorizzazione all'assunzione concessa soltanto dal personale espressamente facoltizzato secondo il vigente sistema dei poteri e delle deleghe;
 - l'assunzione dei candidati individuati come idonei e per i quali è stata fornita autorizzazione all'inserimento viene effettuata dalle Strutture competenti.
- Segregazione dei compiti tra le diverse Strutture e i diversi soggetti coinvolti nelle varie fasi del processo: *(i)* preselezione, *(ii)* selezione e *(iii)* assunzione.
- Attività di controllo:

- compilazione da parte del candidato, al momento dello svolgimento della selezione, di un'apposita modulistica per garantire la raccolta omogenea delle informazioni sui candidati.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta (tra cui quella standard ad esempio testi, application form, contratto di lavoro, ecc.) anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di selezione e assunzione del personale.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione del processo di selezione e assunzione del personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché eventualmente le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- il personale non può dare a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1.;
- qualora il processo di assunzione riguardi:
 - personale diversamente abile, il reclutamento dei candidati avverrà nell'ambito delle liste di soggetti appartenenti alle categorie protette, da richiedere al competente Ufficio del Lavoro;
 - lavoratori stranieri, il processo dovrà garantire il rispetto delle leggi sull'immigrazione del Paese ove è sita l'unità organizzativa di destinazione e la verifica del possesso, per tutta la durata del rapporto di lavoro, dei permessi di soggiorno, ove prescritti;
 - ex dipendenti pubblici, il processo dovrà garantire il rispetto dei divieti di legge.
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere

apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;

- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- promettere o dare seguito a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio alla SGR;
- promettere o dare seguito a richieste di assunzioni di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la SGR ovvero di soggetti da questi indicati, al fine di favorire indebitamente il perseguimento di interessi della SGR con nocimento della società.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.3 Area sensibile concernente i reati societari

7.3.1 Fattispecie di reato

Premessa

L'art. 25-ter del Decreto contempla quasi tutti i reati societari previsti dal Titolo XI del codice civile, che sono qualificabili come reati generali, in quanto non specificamente riferibili all'esercizio della specifica attività della SGR¹⁸.

I reati societari considerati hanno ad oggetto differenti ambiti, tra i quali assumono particolare rilevanza la formazione del bilancio, le comunicazioni esterne, talune operazioni sul capitale, l'impedito controllo e l'ostacolo all'esercizio delle funzioni di vigilanza, fattispecie accomunate dalla finalità di tutelare la trasparenza dei documenti contabili e della gestione societaria e la corretta informazione ai soci, ai terzi e al mercato in generale.

Per quanto concerne le fattispecie criminose che si riferiscono ai documenti contabili e ai controlli delle Autorità di Vigilanza, si rileva che la SGR - anche in quanto appartenente al gruppo bancario Intesa Sanpaolo, la cui Capogruppo è una società quotata - si pone in una posizione privilegiata dal punto di vista della prevenzione e della corretta attuazione dei precetti normativi, in quanto quest'ultima risulta destinataria di una disciplina speciale che impone la procedimentalizzazione dell'intera fase di elaborazione di detta documentazione nonché una serie di obblighi e adempimenti in relazione ai rapporti con le Autorità, con la conseguenza che le modalità di gestione del rischio dei reati qui considerati risultano replicare comportamenti già consolidati nella prassi della SGR o, comunque, derivanti dall'applicazione delle norme primarie e regolamentari vigenti.

Si elencano qui di seguito le fattispecie richiamate dall'art. 25-ter del Decreto.

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

Questi reati si realizzano tramite condotte che, con riferimento alla situazione economica, patrimoniale o finanziaria della società o del gruppo, consistono nella consapevole:

¹⁸ L'art. 25-ter è stato modificato dalla:

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

- esposizione di fatti materiali non rispondenti al vero nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico;
- ovvero l'omissione di fatti materiali rilevanti la cui comunicazione è imposta dalla legge.

In ogni caso, la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto e deve essere idonea a concretamente indurre i destinatari in errore. Inoltre, l'illecito sussiste anche se si riferisce a beni posseduti o amministrati dalla società per conto terzi.

Quando il falso attiene a società diverse da quelle quotate o da quelle ad esse equiparate¹⁹:

- l'esposizione di fatti materiali falsi costituisce il reato in questione solo se contenuta in comunicazioni sociali previste dalla legge e i fatti sono rilevanti;
- si applicano pene attenuate e la causa di esclusione della punibilità per l'ipotesi di particolare tenuità del fatto²⁰.

Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 27 D.Lgs. n. 39/2010)

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, circa la situazione economica, patrimoniale o finanziaria della Società sottoposta a revisione, al fine di conseguire per sé o per altri un ingiusto profitto, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni.

L'illecito è più severamente sanzionato se: ha cagionato un danno patrimoniale ai destinatari delle comunicazioni; concerne la revisione di determinati Enti qualificati dal predetto Decreto "di interesse pubblico" (tra cui le società quotate, gli emittenti di strumenti finanziari diffusi tra il pubblico in maniera rilevante, le banche, alcune imprese di assicurazione, le SIM, le SGR, le SICAV, gli intermediari finanziari di cui all'art. 107 T.U.B.); è commesso per denaro o altra utilità; è commesso in concorso con gli esponenti della società sottoposta a revisione.

Soggetti attivi sono *in primis* i responsabili della società di revisione (reato proprio). E' altresì prevista la punibilità di chi dà o promette il denaro o l'utilità e dei direttori generali, dei componenti

¹⁹ Alle società quotate in un mercato regolamentato nazionale o dell'Unione europea sono equiparate le società che le controllano, le società emittenti strumenti finanziari per i quali è stata chiesta l'ammissione alla negoziazione in detti mercati o che sono negoziati in un sistema multilaterale di negoziazione italiano, nonché le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

²⁰ Si veda l'art. 2621-bis del codice civile che prevede pene inferiori se i fatti sono di lieve entità, in considerazione della natura e delle dimensioni della società e delle modalità o degli effetti della condotta, oppure se i fatti riguardano le piccole società non sottoponibili a procedura fallimentare. In quest'ultimo caso il reato è procedibile solo a querela. Inoltre, l'art. 2621-ter del codice civile richiama l'applicabilità dell'art. 131-bis del codice penale che esclude la punibilità quando, per le modalità della condotta e per l'esiguità del danno o del pericolo, l'offesa è di particolare tenuità e il comportamento non risulti abituale.

l'organo amministrativo e dell'organo di controllo degli enti di interesse pubblico, che abbiano concorso a commettere il fatto.

Tale fattispecie attualmente non costituisce reato presupposto della responsabilità degli enti²¹.

Impedito controllo (art. 2625, comma 2 c.c.)

Il reato di cui all'art. 2625 comma 2 del codice civile si verifica nell'ipotesi in cui gli amministratori impediscano od ostacolano, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri Organi societari, procurando un danno ai soci. Il reato è punito a querela della persona offesa e la pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.

La fattispecie di impedito controllo nei confronti della società di revisione, in origine pure prevista dall'art. 2625 c.c.²², attualmente non costituisce reato presupposto della responsabilità degli enti.

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

La condotta tipica prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche mediante il compimento di operazioni simulate, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

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

²¹ L'art. 25 ter del D. Lgs. 231/2001 continua tuttora a richiamare l'art. 2624 c.c., che in origine prevedeva questo reato, nonostante l'evoluzione normativa nel frattempo intervenuta. Difatti:

- la L. n. 262/2005 introdusse l'art. 174-bis del T.U.F. che puniva con una autonoma fattispecie le falsità nella revisione delle società quotate, delle società da queste controllate e delle società che emettono strumenti finanziari diffusi fra il pubblico in misura rilevante;
- sia l'art. 2624 c.c., sia l'art. 174-bis del T.U.F. a seguito della riforma della disciplina della revisione legale dei conti, sono stati abrogati e, a decorrere dal 7.4.2010, le falsità nella revisione sono punite dalla nuova fattispecie prevista dall'art. 27 del D. Lgs. n. 39/2010.

Tale evoluzione ha fatto sorgere seri dubbi sulla permanente configurabilità della responsabilità degli enti per le condotte in questione. La Corte di Cassazione, con la sentenza n. 34476/2011 delle Sezioni Unite penali, ha ritenuto che il reato di falso in revisione legale quale ora previsto dall'art. 27 del D. Lgs. n. 39/2010 non rientri più nell'ambito di applicazione della responsabilità amministrativa degli enti, in quanto tale norma non è richiamata dall'art. 25-ter del D. Lgs. 231/2001. Va altresì considerato che determinate condotte corruttive nei confronti dei revisori dei conti sono previste e punite ai sensi degli artt. 28 e 30 del D. Lgs. n. 39/2010, ma non costituiscono reato presupposto della responsabilità degli enti.

²² L'art. 2625 c.c. contemplava anche il reato di impedito controllo degli amministratori nei confronti della società di revisione. A seguito della riforma della disciplina della revisione legale dei conti il reato è stato espunto dall'art. 2625 c.c. e riformulato dall'art. 29 del D. Lgs. n. 39/2010, in vigore dal 7.4.2010, che prevede la procedibilità d'ufficio e sanzioni più gravi se viene procurato un danno ai soci e a terzi, o nel caso di revisione legale di enti di interesse pubblico. Poiché l'art. 25-ter del D. Lgs. n. 231/2001 non è stato conseguentemente modificato con l'inserimento di un richiamo anche al citato art. 29, sembra potersi affermare che il reato di impedito controllo nei confronti della società di revisione non configuri più reato presupposto ai fini della responsabilità amministrativa degli enti. Al riguardo sembra valere il medesimo principio di cui alla sentenza della Corte di Cassazione citata nella nota 21.

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

Il reato in questione si perfeziona con l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Si fa presente che se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

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

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

Questo reato si perfeziona quando l'amministratore di una società con titoli quotati in un mercato regolamentato italiano o dell'Unione Europea o diffusi in misura rilevante tra il pubblico, ovvero soggetta a vigilanza ai sensi del Testo Unico Bancario, del Testo Unico dell'Intermediazione Finanziaria o delle norme disciplinanti le attività assicurative o le forme pensionistiche complementari, non comunica, nelle forme e nei termini previsti dall'art. 2391 c.c., all'organo al quale partecipa ovvero alla società e comunque al Collegio Sindacale, l'interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società in questione, ovvero se si tratta di amministratore delegato non si astiene dall'operazione cagionando in tal modo un danno alla società o a terzi.

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

Tale reato si perfeziona nel caso in cui gli amministratori e i soci conferenti formino o aumentino fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni

o quote, sopravvalutazione rilevante dei conferimenti dei beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Il reato si perfeziona con la ripartizione da parte dei liquidatori di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

Integra il reato la condotta di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci, liquidatori, nonché dei soggetti sottoposti alla direzione o vigilanza dei medesimi che, avendo accettato per sé o per altri denaro o altra utilità, o la relativa promessa, compiono od omettono un atto contrario agli obblighi inerenti al loro ufficio o agli obblighi di fedeltà, cagionando nocimento alla società.

Il comma 3 punisce anche la condotta del corruttore (c.d. reato di corruzione tra privati attiva), con le medesime pene previste per i corrotti. Solo tale reato, e non anche quello commesso dai corrotti, costituisce presupposto della responsabilità amministrativa degli enti, se commesso nell'interesse dell'ente al quale il corruttore appartiene.

Il reato è perseguibile a querela della società parte offesa; si procede d'ufficio se dal fatto derivi una distorsione della concorrenza nell'acquisizione di beni o servizi.

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

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Aggiotaggio (art. 2637 c.c.)

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

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Il reato in questione si realizza nel caso in cui, col fine specifico di ostacolare l'attività delle autorità pubbliche di vigilanza, si espongano in occasione di comunicazioni ad esse dovute in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero si occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che si era tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi.

Il reato si perfeziona altresì mediante qualsiasi condotta attiva od omissiva che in concreto determini un ostacolo allo svolgimento delle funzioni demandate alle Autorità di Vigilanza.

La pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.

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

L'art. 173-*bis* del D.Lgs. n. 58/1998 punisce la condotta di chi espone false informazioni od occulta dati o notizie nei prospetti richiesti ai fini della sollecitazione al pubblico risparmio o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio.

Affinché tale condotta integri gli estremi del reato, è indispensabile che il soggetto che la pone in essere agisca con l'intenzione di ingannare i destinatari dei prospetti, al fine di conseguire un ingiusto profitto, per sé o per altri. Occorre altresì che le informazioni false od omesse siano idonee ad indurre in errore i loro destinatari.

Tale fattispecie attualmente non costituisce reato presupposto della responsabilità degli enti²³.

7.3.2 Attività aziendali sensibili

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

- Gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione;
- Gestione dell'informativa periodica;
- Predisposizione dei prospetti informativi;
- Acquisto, gestione e cessione di partecipazioni;

²³ L'art. 25-*ter* del D. Lgs. n. 231/2001 continua tuttora a richiamare l'art. 2623 c.c., che in origine prevedeva questo reato. La L. n. 262/2005 abrogò la norma e introdusse l'attuale fattispecie di falso in prospetto di cui all'art. 173-bis del D.Lgs. n. 58/1998. Poiché l'art. 25-*ter* non è stato conseguentemente modificato, sembra potersi affermare che il reato di falso in prospetto non configuri più reato presupposto ai fini della responsabilità amministrativa degli enti. Al riguardo sembra valere il medesimo principio di cui alla sentenza della Corte di Cassazione citata nella nota 18.

- Gestione dei rapporti con le Autorità di Vigilanza.

Si riportano di seguito, per le prime quattro sopraelencate attività sensibili, i protocolli che dettano i principi di controllo e di comportamento applicabili a dette attività che si completano con la normativa aziendale di dettaglio che regola le attività medesime.

Per quanto concerne il reato di corruzione tra privati, trattandosi di fattispecie a potenziale impatto trasversale su tutte le attività della SGR, si rimanda altresì alle attività sensibili già oggetto dei seguenti protocolli:

- Gestione dei contenziosi e degli accordi transattivi;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del processo di selezione e assunzione di personale;
- Gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione.

in quanto contenenti principi che esplicano la loro efficacia preventiva anche in relazione al reato suddetto.

Infine, relativamente all'attività indicata all'ultimo punto (Gestione dei rapporti con le Autorità di Vigilanza) si rimanda al relativo protocollo di cui al capitolo 7.2, avente la specifica finalità di prevenire, oltre al reato di corruzione, anche il reato societario di cui all'art. 2638 c.c.

Detti protocolli si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

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

Premessa

Il presente protocollo si applica ai membri del Consiglio di Amministrazione e a tutti gli Organi e le Strutture coinvolti nella gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione in occasione di verifiche e di controlli svolti in ottemperanza alle prescrizioni di legge.

Ai sensi del D.Lgs n. 231/2001, il processo in oggetto potrebbe presentare occasioni per la commissione del reato di “impedito controllo”, ai sensi dell’art. 2625 del codice civile nonché dei reati di cui all’art. 27 del D.Lgs. n. 39/2010 (per quanto concerne la fattispecie di false relazioni o comunicazioni da parte dei responsabili della revisione, commessa in concorso con gli organi della società sottoposta a revisione) e all’art. 29 del medesimo Decreto (concernente la fattispecie di impedimento od ostacolo alle attività di revisione legale), che – nonostante il principio affermato dalla Corte di Cassazione e di cui si è dato conto nel precedente paragrafo 7.3.1 – vengono comunque tenuti in considerazione ai fini del presente protocollo.

Limitatamente alla gestione dei rapporti con la Società di Revisione, sussiste altresì il rischio della commissione del reato di “corruzione tra privati”, introdotto dalla L. n. 190/2012 tra i reati societari e descritto nel Capitolo 7.3.

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti in oggetto.

Descrizione del processo

Nell’ambito dell’attività di verifica propria del Collegio Sindacale e della Società di Revisione, la gestione dei rapporti con tali soggetti si articola nelle seguenti attività:

- comunicazione delle informazioni periodiche previste;
- comunicazione di informazioni e di dati societari e messa a disposizione della documentazione, sulla base delle richieste ricevute.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo si basa sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare, i rapporti con il Collegio Sindacale e la Società di Revisione, sono intrattenuti dal Responsabile della Struttura di riferimento o dai soggetti dal medesimo appositamente incaricati.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Collegio Sindacale e la Società di Revisione al fine di garantire, per tutte le fasi del processo, un meccanismo di maker e checker.
- Partecipazione regolare e continua del Collegio Sindacale alle riunioni del Consiglio di Amministrazione, a garanzia della effettiva conoscenza da parte dell'Organo di Controllo in merito alle scelte di gestione della SGR.
- Tempestiva e completa evasione delle richieste di documentazione specifica avanzate dal Collegio Sindacale - anche per il tramite della Struttura Affari Societari (della Controllante) - nell'espletamento della propria attività di vigilanza e controllo.
- Tempestiva e completa evasione, a cura delle strutture competenti, delle richieste di documentazione specifica avanzate dalla Società di Revisione nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili: ciascuna Struttura ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori.

- Tempestiva e completa messa a disposizione della Società di Revisione, da parte delle strutture interessate, della documentazione disponibile relativa alle attività di controllo e ai processi operativi seguiti, sui quali i revisori effettuano le proprie attività di verifica.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo del Collegio Sindacale;
 - verifica e conservazione delle dichiarazioni di supporto per la predisposizione delle Representation Letter, con firma delle stesse da parte dell'Amministratore Delegato/Direttore Generale, rilasciate alla Società di Revisione;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla gestione dei rapporti con il Collegio Sindacale e la Società di Revisione.

Principi di comportamento

Le Strutture e gli Organi della SGR, a qualsiasi titolo coinvolte nella gestione dei rapporti con il Collegio Sindacale e la Società di Revisione, sono tenute alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità e al pieno rispetto del ruolo istituzionale degli stessi, dando puntuale e sollecita esecuzione alle prescrizioni e agli eventuali adempimenti richiesti nel presente protocollo, in conformità alle disposizioni di legge esistenti in materia nonché alle eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- devono essere puntualmente trasmesse le comunicazioni periodiche al Collegio Sindacale, – anche per il tramite della Struttura Affari Societari (della Controllante) - e alla Società di Revisione, e tempestivamente riscontrate le richieste/istanze pervenute dagli stessi;
- i membri del Consiglio di Amministrazione e i dipendenti che, a qualunque titolo, siano coinvolti in una richiesta di produzione di documenti o di informazioni da parte del Collegio Sindacale – per il tramite della Struttura Affari Societari (della Controllante) – nonché della Società di Revisione pongono in essere comportamenti improntati alla massima correttezza e trasparenza e non ostacolano in alcun modo le attività di controllo e/o di revisione;

- i dati e i documenti devono essere resi disponibili in modo puntuale e in un linguaggio chiaro, oggettivo ed esaustivo in modo da fornire informazioni accurate, complete, fedeli e veritiere;
- ciascuna Struttura aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione formalmente prodotta e/o consegnata ai membri del Collegio Sindacale e ai Revisori, nell'ambito della propria attività, ivi inclusa quella trasmessa in via elettronica.

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

- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre il Collegio Sindacale e la Società di Revisione in errore di valutazione tecnico-economica della documentazione presentata;
- promettere o dare somme di denaro o altre utilità a membri del Collegio Sindacale o della Società di Revisione con la finalità di promuovere o favorire interessi della SGR;
- promettere versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore) o accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti alla Società di Revisione della SGR, al fine di favorirne indebitamente gli interessi con nocimento della società stessa, oppure minacciarli di un danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti e affini e, a titolo più generale, tutte le operazioni che comportino la generazione di una perdita per la SGR e la creazione di un utile per i soggetti predetti (es.: applicazione di sconti o condizioni non in linea con i parametri di mercato).

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.3.2.2. Gestione dell'informativa periodica

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della SGR.

Ai sensi del D.Lgs. n. 231/2001, il processo di predisposizione dei documenti in oggetto potrebbe presentare occasioni per la commissione del reato di "false comunicazioni sociali", così come disciplinato agli artt. 2621 e 2622 del Codice Civile. Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati di "corruzione", nelle loro varie tipologie, di "induzione indebita", di "corruzione tra privati", nonché i reati di "riciclaggio" e di "autoriciclaggio".

La Capogruppo è sottoposta a precisi obblighi informativi di bilancio in qualità di società quotata sul mercato regolamentato italiano. Il processo di predisposizione dei documenti in oggetto è pertanto disciplinato da apposito Regolamento approvato dal Consiglio di Gestione di Intesa Sanpaolo S.p.A. con parere favorevole del Consiglio di Sorveglianza, in risposta alle sollecitazioni provenienti dall'art. 154-bis del TUF, che ha qualificato normativamente la figura del "Dirigente Preposto alla redazione dei documenti contabili societari" prevedendo specifiche responsabilità funzionali a garantire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria del Gruppo.

La Controllante FIDEURAM – Intesa Sanpaolo Private Banking ha recepito le "*Linee Guida di Governo Amministrativo Finanziario*" di Intesa Sanpaolo, da ultimo, con delibera del Consiglio di Amministrazione del 12 maggio 2008 e, in quanto destinataria diretta della disciplina di cui all'art. 154-bis del TUF, ha successivamente approvato, con delibera del 14 ottobre 2008, il *Regolamento "Governo Amministrativo Finanziario"* di FIDEURAM – Intesa Sanpaolo Private Banking, volto a regolare – in attuazione delle regole di indirizzo e coordinamento contenute nelle Linee Guida della Capogruppo – il funzionamento del processo di verifica dell'adeguatezza ed effettiva applicazione delle procedure amministrative e contabili in FIDEURAM – Intesa Sanpaolo Private Banking e presso le sue controllate.

La sopra richiamata normativa, recepita dal Consiglio di Amministrazione di Fideuram Investimenti SGR S.p.A. con delibera del 30/3/2009, definisce i principi di riferimento, i ruoli e le responsabilità attribuite alle Strutture della Controllante e della SGR in relazione al processo afferente il presente Protocollo, di cui deve intendersi parte integrante. Il Regolamento prevede, in particolare, che le procedure sensibili ai fini dell'informativa finanziaria siano oggetto di formalizzazione e di verifica, al fine di pervenire alla valutazione della loro adeguatezza richiesta dal citato art. 154-bis del TUF, garantendone l'affidabilità e, in particolare, il presidio dei sistemi di controllo interno funzionali alla formazione del bilancio e di ogni altra comunicazione di ordine finanziario a livello di Gruppo; tali procedure rappresentano pertanto le regole operative di dettaglio del presente protocollo.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Nell'ambito dei processi sensibili ai fini dell'informativa finanziaria, particolare rilievo assumono le attività strettamente funzionali alla produzione del bilancio d'esercizio, delle situazioni contabili infrannuali, dei Rendiconti dei Fondi Comuni di Investimento e l'alimentazione del reporting package per il bilancio consolidato del Gruppo, la determinazione degli oneri fiscali e lo svolgimento degli adempimenti relativi alle imposte dirette e indirette. Tali attività attengono ai seguenti processi aziendali:

- Gestione della contabilità e delle segnalazioni di vigilanza;
- Gestione del bilancio d'impresa e del reporting package per il bilancio consolidato del Gruppo;
- Redazione dei Rendiconti dei Fondi Comuni di Investimento;
- Gestione degli adempimenti fiscali.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

I documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della SGR, nonché i Rendiconti dei Fondi Comuni di Investimento gestiti dalla stessa, sono redatti in base alle specifiche procedure, prassi e logiche aziendali e di Gruppo in essere che:

- identificano con chiarezza e completezza le funzioni interessate nonché i dati e le notizie che le stesse devono fornire;
- identificano i criteri per le rilevazioni contabili dei fatti aziendali e per la valutazione delle singole poste;
- determinano le scadenze, gli argomenti oggetto di comunicazione e informativa, l'organizzazione dei relativi flussi e l'eventuale richiesta di rilascio di apposite attestazioni;
- prevedono la trasmissione di dati e informazioni alla Struttura responsabile della raccolta attraverso un sistema che consente la tracciabilità delle singole operazioni e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- prevedono criteri e modalità per l'elaborazione dei dati della SGR necessari per la formazione del bilancio consolidato del Gruppo e la trasmissione degli stessi alla Controllante.

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti:
 - ogni singola Struttura è responsabile dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essa demandate e degli eventuali commenti in bilancio di propria competenza;
 - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in relazione alle attività in oggetto, in particolare per quanto riguarda il passaggio a perdite;
 - sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
 - la verifica dell'adeguatezza dei processi sensibili ai fini della informativa contabile e finanziaria nonché dei relativi controlli è affidata ad una specifica Struttura della

Controllante FIDEURAM – Intesa Sanpaolo Private Banking, in staff al Dirigente Preposto che rappresenta altresì l'interfaccia del Servizio di Governance Amministrativo Finanziaria della Capogruppo con il quale si coordina per la redazione dei documenti contabili e societari e all'Audit nell'ambito dello svolgimento della sua attività.

- Segregazione delle funzioni:
 - il processo di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della SGR prevede il coinvolgimento di distinte Strutture, operanti nelle diverse fasi del processo in base ai principi riportati nel documento “Linee Guida di governo amministrativo finanziario”.

- Attività di controllo:
 - le attività di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della SGR, nonché dei Rendiconti dei Fondi Comuni di Investimento, sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali. Si riportano nel seguito i principali controlli svolti dalle singole Strutture:
 - verifiche, con cadenza periodica, dei saldi dei conti di contabilità generale, al fine di garantirne la quadratura con i rispettivi partitari;
 - verifica, con periodicità prestabilita, di tutti i saldi dei conti lavorazione, transitori e similari, per assicurare che le Unità interessate che hanno alimentato la contabilità eseguano le necessarie scritture nei conti appropriati;
 - esistenza di controlli maker e checker attraverso i quali la persona che esegue l'operazione è differente da quella che la autorizza, previo controllo di adeguatezza;
 - produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
 - analisi degli scostamenti, attraverso il confronto tra i dati contabili esposti nel periodo corrente e quelli relativi a periodi precedenti;
 - controllo di merito in sede di accensione di nuovi conti e aggiornamento del piano dei conti;
 - quadratura della versione definitiva del bilancio con i dati contabili.
 - La verifica dell'adeguatezza dei processi sensibili ai fini dell'informativa contabile e finanziaria e dell'effettiva applicazione dei relativi controlli è articolata nelle seguenti fasi:
 - verifica del disegno dei controlli;

- test dell'effettiva applicazione dei controlli;
 - identificazione delle criticità e dei piani di azione correttivi;
 - monitoraggio sull'avanzamento e sull'efficacia delle azioni correttive intraprese.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - il processo decisionale, con riferimento sia alle attività di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della SGR che alle attività di redazione dei Rendiconti dei Fondi Comuni di Investimento, è garantito dalla completa tracciabilità di ogni operazione contabile sia tramite sistema informatico sia tramite supporto cartaceo;
 - tutte le scritture di rettifica effettuate dalle singole Strutture responsabili dei conti di propria competenza o dalla Struttura deputata alla gestione del Bilancio, sono supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati e, analiticamente, lo sviluppo dei relativi calcoli;
 - tutta la documentazione relativa ai controlli periodici effettuati viene archiviata presso ciascuna Struttura coinvolta per le voci contabili di propria competenza;
 - tutta la documentazione di supporto alla stesura del bilancio è archiviata presso la Struttura deputata alla gestione del Bilancio e/o presso le strutture coinvolte nel processo di redazione delle disclosures.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nelle attività di tenuta della contabilità e della successiva predisposizione/deposito delle comunicazioni sociali in merito alla situazione economico e patrimoniale della SGR (bilancio di esercizio, relazione sulla gestione, relazioni trimestrali e semestrali, ecc.) e del Gruppo (reporting package per il bilancio consolidato) sono tenute ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia, nonché le norme contenute nelle “Linee Guida di governo amministrativo finanziario” e nelle procedure che disciplinano le attività in questione, norme tutte improntate a principi di trasparenza, accuratezza e completezza delle informazioni contabili al fine di produrre situazioni economiche, patrimoniali e finanziarie veritiere e tempestive anche ai sensi e ai fini di cui agli artt. 2621 e 2622 del Codice Civile. In particolare, le Strutture sono tenute a tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della SGR.

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

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della SGR e del Gruppo;
- omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della SGR e del Gruppo.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.3.2.3. Predisposizione dei prospetti informativi

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella predisposizione dei Prospetti Informativi²⁴ richiesti ai fini della sollecitazione al pubblico risparmio o dell'ammissione alla quotazione nei mercati regolamentati. Il relativo processo potrebbe presentare occasioni per la commissione del reato di "falso in prospetto", così come disciplinato all'art. 173-bis del T.U.F., ed implica evidenti connessioni con le procedure predisposte per la prevenzione delle condotte in tema di abusi di mercato; nonostante sussistano seri dubbi sulla rilevanza del reato di "falso in prospetto" ai fini della responsabilità amministrativa degli Enti, come si è detto nell'illustrazione della fattispecie (paragrafo 7.3.1), si ritiene comunque opportuno prevedere specifici principi di controllo e di comportamento a presidio di tale processo.

Il Prospetto contiene le informazioni che *"a seconda delle caratteristiche dei prodotti finanziari e degli Emittenti, sono necessarie affinché gli investitori possano pervenire a un fondato giudizio sulla situazione patrimoniale, economica e finanziaria, sull'evoluzione dell'attività dell'Emittente, nonché sui prodotti finanziari e sui relativi diritti"*.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di predisposizione dei prospetti informativi, in conformità alla normativa vigente, prevede lo svolgimento delle seguenti fasi:

- raccolta delle informazioni necessarie alla predisposizione dei prospetti presso le Strutture competenti;

²⁴ Ai sensi delle disposizioni previste dal D.Lgs n. 58 del 24/2/1998 e successive modifiche (tra cui la Legge n. 262 del 28/12/2005) e dalla Direttiva 2003/71/CE del 4/11/2003 come recepita nel Regolamento (CE) n. 809/2004 della Commissione del 29 aprile 2004.

I Prospetti Informativi in argomento sono sia quelli relativi alle emissioni sul mercato domestico, sia quelli relativi alle emissioni di titoli sui mercati internazionali.

- redazione e validazione della bozza del prospetto;
- presentazione all'Autorità competente dell'istanza di autorizzazione alla pubblicazione del prospetto;
- predisposizione e sottoscrizione della versione definitiva del prospetto;
- inoltro del prospetto e gestione dei rapporti con l'Autorità competente.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti
 - la SGR identifica le Strutture deputate alla predisposizione e redazione delle Sezioni che compongono i Prospetti Informativi, individuando, nell'ambito delle rispettive mission ovvero tramite delega formale, le Strutture competenti alla compilazione, sottoscrizione e inoltro alle Autorità;
 - i rapporti con le Autorità competenti sono intrattenuti da soggetti dotati di specifiche deleghe in tal senso, nel rispetto dei principi di comportamento sanciti nel protocollo *"Gestione dei rapporti con le Autorità di Vigilanza"*.
- Segregazione dei compiti:
 - il processo di predisposizione dei Prospetti Informativi prevede il coinvolgimento di diverse Strutture, responsabili, relativamente alle specifiche competenze, dell'elaborazione delle informazioni e della redazione dei documenti necessari alla compilazione dei Prospetti medesimi.
- Attività di controllo da parte di ciascuna Struttura competente ed in particolare:
 - controlli di completezza, correttezza ed accuratezza delle informazioni riportate sui documenti di specifica competenza che devono essere supportati da meccanismi di maker e checker;
 - controlli di carattere giuridico sulla conformità alla normativa di riferimento.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- o ciascuna fase rilevante del processo di predisposizione dei Prospetti Informativi deve risultare da apposita documentazione scritta;
- o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti per predisporre i Prospetti Informativi.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nelle attività di predisposizione dei Prospetti Informativi, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare tutte le Strutture coinvolte sono tenute a:

- mantenere un comportamento corretto, trasparente e collaborativo al fine di garantire la tutela del risparmio degli investitori;
- porre la massima attenzione ed accuratezza in ogni attività finalizzata all'acquisizione, elaborazione ed illustrazione di dati e di informazioni relative a prodotti finanziari necessari per permettere agli investitori di formare un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della SGR e del Gruppo;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione dei Prospetti Informativi, i contratti / lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto.

Per la corretta gestione delle informazioni sottese alla emanazione dei Prospetti Informativi, si rimanda altresì ai principi di comportamento sanciti dal protocollo per la *“Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato”*.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di redigere Prospetti Informativi incompleti e/o contenenti dati falsi o alterati.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.3.2.4. Acquisto, gestione e cessione di partecipazioni

Premessa

Il presente protocollo si applica a tutte le strutture della Società coinvolte nell'acquisto, nella gestione e nella cessione di partecipazioni – dirette o indirette, qualificate o non qualificate – al capitale di altre società e ad altre forme di investimento assimilabili all'assunzione di una partecipazione (quali ad esempio, la sottoscrizione di prestiti obbligazionari convertibili o di strumenti finanziari partecipativi).

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di "Corruzione tra privati", nella sua tipologia di corruzione attiva, e di "Omessa comunicazione del conflitto di interessi".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo si articola nelle seguenti fasi:

- esame di fattibilità dell'operazione e/o individuazione delle opportunità di investimento;
- ottenimento del preventivo benestare della Capogruppo e della Controllante FIDEURAM – Intesa Sanpaolo Private Banking ai sensi della vigente normativa interna;
- gestione dei rapporti pre-contrattuali e svolgimento delle attività propedeutiche alla stipula del contratto (verifica adempimenti normativi, *due diligence*, ecc);
- perfezionamento del contratto;
- gestione della partecipazione e degli adempimenti connessi (compresa la proposta di designazione di esponenti presso la società partecipata);
- gestione del disinvestimento.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
 - ai sensi dello Statuto le decisioni concernenti l'assunzione e la cessione di partecipazioni sono riservate all'esclusiva competenza del Consiglio di Amministrazione;
 - i soggetti che esercitano poteri autorizzativi e/o negoziali in ogni fase del processo sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale;
 - gli atti e documenti che impegnano la Società devono essere sottoscritti da soggetti muniti dei necessari poteri;
 - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in tema di partecipazioni; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

- Segregazione dei compiti tra i soggetti coinvolti nel processo al fine di garantire tra le fasi del processo un meccanismo di maker e checker.

- Attività di controllo:
 - verifica dell'istruttoria effettuata secondo quanto previsto dalla normativa interna anche mediante l'eventuale esecuzione di specifiche attività di *due diligence* (ad es. economico/finanziaria, contabile, legale, fiscale, ecc.) sull'impresa oggetto d'investimento (c.d. "impresa target");
 - verifica che la delibera contenga i criteri di valutazione del prezzo dell'operazione secondo le prassi di mercato;
 - verifica del rispetto degli adempimenti legislativi e regolamentari (ad es.: in tema di antiriciclaggio);
 - richiesta di aggiornamento dell'anagrafe di Gruppo delle partecipazioni in essere;
 - verifica del processo di valutazione periodica delle partecipazioni in essere nell'ambito della predisposizione del Bilancio d'impresa..

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - ciascuna fase rilevante dell'attività regolata dal presente protocollo deve risultare da apposita documentazione scritta;
 - ogni accordo/convenzione/contratto/altro adempimento funzionali all'acquisto, gestione e cessione di partecipazioni è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni sottostanti all'istruttoria svolta per l'assunzione della partecipazione e alle scelte effettuate nell'attività di gestione, ciascuna Struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica oggetto del presente protocollo.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture della Società, a qualsiasi titolo coinvolte nel processo di acquisto, gestione e cessione di partecipazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo. In particolare:

- i soggetti che esercitano poteri autorizzativi e/o negoziali in sede pre-contrattuale, contrattuale e di gestione di rapporti partecipativi devono essere individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale;
- la documentazione relativa ai contratti funzionali all'acquisto, gestione e cessione di partecipazioni deve essere conforme alla normativa generale e speciale vigente per il settore di riferimento, anche mediante il ricorso al contributo consulenziale delle competenti funzioni aziendali e/o di professionisti esterni, di Capogruppo e della Controllante FIDEURAM – Intesa Sanpaolo Private Banking;
- il personale non può dare seguito a qualunque richiesta di denaro o altra utilità di cui dovesse essere destinatario o venire a conoscenza formulata da esponenti apicali, o da persone loro subordinate, appartenenti a società controparti o in relazione con la Società, finalizzata al compimento o all'omissione da parte di questi di un atto contrario agli obblighi

inerenti al proprio ufficio o agli obblighi di fedeltà e deve immediatamente segnalare al proprio Responsabile; questi a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza secondo quanto previsto dal Capitolo 4.1.;

- qualora sia previsto il coinvolgimento di soggetti terzi nella stipula e/o nella gestione dei contratti funzionali all'acquisto, gestione e cessione di partecipazioni, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001, e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- il personale designato dalla Società in qualità di componente dell'organo amministrativo di una società partecipata è tenuto a comunicare a quest'ultima - nelle forme e nei termini previsti dall'art. 2391 c.c. - l'interesse che, per conto della Società ovvero per conto proprio o di terzi, abbia in una determinata operazione della società in questione, astenendosi dall'effettuare l'operazione se si tratta di amministratore delegato.

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

- comunicare dati falsi o alterati;
- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società, o a soggetti sottoposti alla direzione o vigilanza dei medesimi al fine di ottenere da parte di questi il compimento o l'omissione di un atto contrario agli obblighi inerenti il loro ufficio o agli obblighi di fedeltà con la finalità di promuovere o favorire interessi della Società. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti (es.: applicazioni di sconti o condizioni non in linea con i parametri di mercato);

- affidare incarichi a consulenti esterni eludendo criteri documentabili e obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.4 Area sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona

7.4.1 Fattispecie di reato

Premessa

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

Il settore finanziario - e con esso, la politica del Gruppo Intesa Sanpaolo - ha da sempre dedicato particolare attenzione e impegno nella collaborazione alla prevenzione di fenomeni criminali nel mercato finanziario e al contrasto al terrorismo, impegno questo che la SGR assume anche ai fini della tutela della sana e prudente gestione, della trasparenza e correttezza dei comportamenti e del buon funzionamento del sistema nel suo complesso. Inoltre, nell'esercizio delle attività finanziarie è di particolare evidenza il rischio di mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi, risorse finanziarie o disponibilità economiche che risultino strumentali al perseguimento di attività illecite.

Si fornisce qui di seguito una sintetica esposizione delle categorie di fattispecie in questione.

* * *

Sezione I - Delitti con finalità di terrorismo o eversione dell'ordine democratico

L'art. 25-*quater* del decreto dispone la punibilità dell'Ente, ove ne sussistano i presupposti, nel caso in cui siano commessi, nell'interesse o a vantaggio dell'Ente stesso, delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale, dalle leggi speciali o in violazione della Convenzione internazionale per la repressione del finanziamento del terrorismo, firmata a New York il 9.12.1999.

La norma non prevede un elenco di reati chiuso e tassativo, ma si riferisce ad un qualsivoglia illecito penale caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico perseguita dal soggetto agente²⁵.

Si menzionano di seguito le principali fattispecie applicabili.

A) Delitti con finalità di terrorismo o eversione dell'ordine democratico previsti dal codice penale o da leggi penali speciali.

Si tratta dei delitti politici, cioè contro la personalità interna e internazionale dello Stato, contro i diritti politici del cittadino, nonché contro gli Stati esteri, i loro Capi e i loro rappresentanti.

Le fattispecie di maggior rischio, in quanto potrebbero astrattamente presentarsi nello svolgimento dell'attività della Società, sono quelle concernenti la "Partecipazione a prestiti a favore del nemico" (art. 249 c.p.), il "Sequestro di persona a scopo di terrorismo o di eversione" (art. 289 bis c.p.) e il reato di cui all'art. 270 bis c.p., denominato "Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico". In particolare, tale ultima fattispecie punisce anche qualsiasi forma di finanziamento a favore di associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione.

Si richiama inoltre l'attenzione sui reati a danno del patrimonio, ed in particolare sulle fattispecie di riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, beninteso qualora commessi strumentalmente al perseguimento di finalità di terrorismo o eversione dell'ordine democratico.

Accanto alle disposizioni del codice penale, vengono in considerazione i reati previsti in leggi speciali attinenti alle più varie materie (ad. es. in materia di armi, di stupefacenti, di tutela ambientale, ecc.) nonché in tutta quella parte della legislazione italiana, emanata negli anni '70 e '80, volta a combattere il terrorismo (ad es. in tema di sicurezza della navigazione aerea e marittima, ecc.).

B) Delitti con finalità di terrorismo previsti dalla Convenzione di New York del 1999.

Il richiamo a tale Convenzione operato dall'art. 25-*quater*, comma 4, del Decreto tende chiaramente ad evitare possibili lacune nella disciplina imperniata non sulla tipologia di reato, ma

²⁵ L'art. 270-sexies c.p. considera connotate da finalità di terrorismo le condotte che possono arrecare grave danno ad un Paese o a un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o ad astenersi dal compiere un qualsiasi atto, o di destabilizzare le strutture politiche fondamentali, costituzionali, economiche e sociali, nonché le altre condotte previste da convenzioni o da norme internazionali. Secondo la giurisprudenza (Cassazione penale n. 39504/2008) l'espressione "eversione dell'ordine democratico" non può essere limitata al solo concetto di azione politica violenta, ma deve intendersi riferita all'ordinamento costituzionale, e quindi ad ogni mezzo di lotta politica che tenda al sovvertimento del sistema democratico e costituzionale esistente o alla deviazione dai principi fondamentali che lo governano.

sulla finalità perseguita, ed è dunque diretto a coprire ogni fattispecie residua anche mediante il rinvio ad atti internazionali.

* * *

Sezione II - Delitti di criminalità organizzata

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

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

Con riferimento alle fattispecie di associazioni per delinquere sopra considerate, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione a un'associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) dei reati che costituiscono il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un esponente o di un dipendente dell'Ente potrebbe determinare la responsabilità amministrativa dell'Ente stesso, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio dell'Ente medesimo. E' inoltre richiesto che il vincolo associativo si espliciti attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta cioè l'occasionale accordo per la commissione di uno o più delitti determinati. La giurisprudenza ritiene altresì possibile il concorso nel reato di associazione criminosa da parte di colui che, pur non partecipando all'associazione stessa, fornisca un apporto sostanziale, anche se episodico, alla sua sussistenza od al perseguimento dei suoi scopi.

L'associazione di tipo mafioso (art. 416-bis c.p.) si distingue dalla associazione per delinquere generica per il fatto che coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, oppure - anche non mediante la commissione di delitti, ma pur sempre con l'uso del metodo mafioso - per acquisire in modo diretto od indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per

realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

La norma si applica anche alla camorra e alle altre associazioni, comunque denominate, anche straniere, che presentino i connotati mafiosi predetti. Lo scambio elettorale politico-mafioso invece è commesso da chi propone o accetta la promessa di procurare voti con l'uso del metodo mafioso in cambio dell'erogazione o della promessa di denaro o di altra utilità.

Gli altri due tipi di associazioni criminose sono invece caratterizzate dall'essere preordinate al fine della commissione degli specifici reati in esse considerati, vale a dire: dei reati in tema di schiavitù, di tratta di persone e di immigrazione clandestina (puniti ai sensi degli artt. 600, 601 e 602 c.p. nonché dell'art. 12 comma 3-bis del D. Lgs. n. 286/1998) e dei reati di illecita produzione, traffico o detenzione di sostanze stupefacenti o psicotrope. Questi specifici reati-fine (eccetto quelli in materia di stupefacenti) costituiscono di per sé autonomi reati presupposto della responsabilità dell'Ente, come meglio si dirà nel prosieguo a proposito dei reati contro la persona e dei reati transnazionali.

L'art. 24-ter prevede inoltre la generica categoria dei delitti di qualsivoglia tipo, commessi avvalendosi del metodo mafioso od al fine di favorire l'attività di una associazione mafiosa, fermo restando, per la responsabilità dell'Ente, il requisito dell'interesse o del vantaggio del medesimo.

La prima circostanza si ritiene ricorra allorché il soggetto agente, pur senza appartenere al sodalizio criminoso o concorrere con esso, pone in essere una condotta idonea ad esercitare una particolare intimidazione, quale ad esempio la minaccia avvalendosi dello sfruttamento della "fama" di organizzazioni criminali operanti nell'ambito di un determinato territorio. L'ipotesi della commissione di un reato di qualsiasi tipo atto ad agevolare l'attività di una associazione mafiosa si verifica quando il soggetto abbia agito con tale scopo specifico e la sua condotta sia concretamente idonea a realizzare tale risultato, come ad esempio nel caso del reato di riciclaggio compiuto essendo a conoscenza della riferibilità dell'operazione ad una associazione mafiosa.

Infine, ai sensi del medesimo art. 24-ter, rilevano i seguenti reati, solitamente, anche se non necessariamente, realizzati nell'ambito di organizzazioni criminali.

Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.).

Il reato consiste nel sequestro di una persona con lo scopo di conseguire per sé o per altri un ingiusto profitto in cambio della liberazione. Il profitto potrebbe anche consistere in un vantaggio di natura non patrimoniale. In casi particolari potrebbero essere ritenuti corresponsabili del reato anche coloro che, pur non avendo partecipato al sequestro, si attivino per far sì che gli autori possano conseguire il riscatto, contribuendo al protrarsi delle trattative e conseguentemente, della privazione della libertà personale del sequestrato, o al conseguimento del profitto da parte dei sequestratori. Potrebbe invece integrare il reato di riciclaggio l'attività di chi interviene nel

trasferimento, nella circolazione o nell'impiego di somme di denaro o di altri beni, essendo a conoscenza della provenienza dal reato in questione.

Delitti in tema di armi e di esplosivi (art. 407 comma 2, lettera a), n. 5 c.p.p.).

Si tratta di fattispecie previste dalle leggi speciali vigenti in materia (in particolare dalla L. n. 110/1975 e dalla L. n. 895/1967), che puniscono le condotte di illegale fabbricazione, introduzione nello Stato, vendita, cessione, detenzione e porto abusivo di esplosivi, di armi da guerra e di armi comuni da sparo, con esclusione di quelle da bersaglio da sala, o ad emissione di gas, o ad aria compressa. Anche in questo caso, come per il reato precedente, eventuali collusioni in qualsiasi forma dei dipendenti della SGR con gli autori dei reati in questione, con la consapevolezza di anche solo indirettamente favorirli, potrebbe comportare il concorso nei reati stessi o l'imputabilità per altri reati, quali ad esempio il riciclaggio.

* * *

Sezione III - Delitti transnazionali

La responsabilità degli Enti per tale categoria di reati è sancita dalla L. n. 146/2006, al fine di più efficacemente contrastare le organizzazioni criminali che agiscono a livello internazionale.

Si considera transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato e:

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

Si descrivono di seguito le fattispecie penali che, se integrate dagli elementi costitutivi dell'interesse o del vantaggio dell'Ente e della transnazionalità (sui quali pure si ritiene debba sussistere la consapevolezza da parte del soggetto agente), possono dar luogo alla responsabilità dell'Ente.

Associazioni per delinquere previste dagli artt. 416 e 416-bis c.p. ovvero finalizzate al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. n. 43/1973) o al traffico di stupefacenti (art. 74 D.P.R. n. 309/1990)

Per la definizione delle condotte di base dei reati associativi in questione si rimanda a quanto sopra osservato a proposito dei delitti di criminalità organizzata. Si ritiene che, ricorrendo le caratteristiche della transnazionalità, siano applicabili all'Ente unicamente le sanzioni previste dalla L. n. 146/2006 e non anche quelle di cui all'art. 24-ter del Decreto.

Reati in tema di immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5 del D. Lgs. n. 286/1998)

La norma punisce le condotte consistenti nel trasportare illegalmente stranieri nel territorio dello Stato, nel promuovere, dirigere, organizzare o finanziare tale trasporto, oppure in altri atti diretti a procurare illegalmente l'ingresso di stranieri nel territorio italiano o di uno Stato diverso da quello di loro appartenenza o residenza permanente. E' però richiesto che ricorra almeno una delle cinque condizioni elencate dalla norma stessa²⁶.

Le medesime condotte sono punite più severamente se si verifici la contemporanea presenza di almeno due delle cinque condizioni predette oppure se siano commesse con determinate finalità, quali: il reclutamento di persone destinate alla prostituzione; lo sfruttamento sessuale o lavorativo, lo sfruttamento di minori, o in genere, la finalità di trarre un profitto anche indiretto.

Infine, il comma 5 punisce il favoreggiamento della permanenza dello straniero al fine di trarre un ingiusto profitto dalla sua condizione di illegalità. Si deve ritenere che l'ingiusto profitto sussista quando l'equilibrio delle prestazioni sia fortemente alterato, quale conseguenza dello sfruttamento da parte del soggetto agente dello stato di clandestinità, da lui conosciuto.

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)

Il reato è commesso da chi, con violenza o minaccia o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci coloro che siano chiamati a rendere dichiarazioni davanti all'autorità giudiziaria, utilizzabili in un procedimento penale, e abbiano la facoltà di non rispondere.

Si precisa che tale reato può dar luogo alla responsabilità dell'Ente anche se commesso senza le caratteristiche della transnazionalità, essendo richiamato, oltre che dalla Legge n. 146/2006, anche dall'art. 25-decies del Decreto.

²⁶ In sintesi: a) procurato ingresso o permanenza illegale di cinque o più persone; b) pericolo per l'incolumità delle persone trasportate; c) loro trattamento degradante; d) fatti commessi da tre o più persone concorrenti o con utilizzo di servizi di trasporto internazionali o di documenti falsi o illegalmente ottenuti; e) fatti commessi da chi è nella disponibilità di armi o di esplosivi.

Favoreggiamento personale (art. 378 c.p.)

La condotta criminosa consiste nel prestare aiuto a taluno - dopo l'avvenuta commissione di un delitto per il quale la legge stabilisce l'ergastolo o la reclusione e fuori dei casi di concorso nel medesimo - ad eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa. Il reato sussiste anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto. La pena è aggravata quando il delitto commesso è quello di associazione mafiosa.

Si precisa che, per giurisprudenza maggioritaria, integrano il reato anche le false risposte, tese ai fini di cui sopra, alle richieste dell'Autorità Giudiziaria.

* * *

Sezione IV - Delitti contro la persona

L'art. 25-*quinquies* del Decreto elenca talune fattispecie di reato poste a presidio della personalità individuale previste dal codice penale con il fine di contrastare aspramente il fenomeno delle "nuove schiavitù" quali prostituzione, tratta degli esseri umani, sfruttamento dei minori, accattonaggio, attività strettamente collegate al proliferare della criminalità organizzata e delle "nuove mafie".

In particolare, sono contemplate le fattispecie delittuose qui di seguito elencate: **“Riduzione o mantenimento in schiavitù” (art. 600 c.p)**, **“Prostituzione minorile” (art. 600-bis c.p.)**, **“Pornografia minorile” (art. 600-ter c.p.)**, **“Detenzione di materiale pornografico” (art. 600-quater c.p.)**, **“Iniziativa turistiche volte allo sfruttamento della prostituzione minorile” (art. 600-quinquies c.p.)**, **“Adescamento di minorenni” (art. 609-undecies c.p.)**, **“Tratta di persone” (art. 601 c.p.)**, **“Acquisto e alienazione e di schiavi” (art. 602 c.p.)**.

Infine, si ricorda che l'art. 25-quater 1 dispone la punibilità dell'Ente nel caso di commissione del reato contro la persona di cui all'art. 583-bis c.p. (Pratiche di mutilazione degli organi genitali femminili).

Il rischio di responsabilità per i delitti in questione si può ritenere rilevante solo con riferimento all'ipotesi in cui un esponente o un dipendente della SGR agiscano in concorso con l'autore materiale del reato. La forma di concorso che presenta maggiori profili di rischio è quella connessa alla messa a disposizione di risorse finanziarie o economiche in favore di organizzazioni o di soggetti che pongano in essere reati dei tipi sopra menzionati.

Tra i reati di questa Sezione – anche se è evidente il nesso col reato transnazionale di sfruttamento di lavoratori clandestini di cui alla precedente Sezione - può collocarsi il delitto

richiamato dall'art. 25-duodecies del Decreto²⁷, di **“Impiego di cittadini di paesi terzi il cui soggiorno è irregolare”** (art. 22, comma 12-bis, del D. Lgs. n. 286/1998 - Testo Unico sull'immigrazione), che punisce i datori di lavoro che assumano o si avvalgano di dipendenti extracomunitari privi di permesso di soggiorno, ovvero scaduto senza che sia richiesto il rinnovo, revocato, o annullato. La responsabilità dell'ente è prevista solo al ricorrere di determinate circostanze aggravanti²⁸. Benché il rischio della commissione di tale reato nell'ambito della SGR appaia remoto, si rende comunque opportuno averne debita considerazione nel contesto della gestione del processo di selezione e assunzione del personale e delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

7.4.2 Attività aziendali sensibili

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

Le attività sopra individuate sono le medesime nelle quali è più alto il rischio che si verifichino anche reati di riciclaggio. Pertanto, ai fini della prevenzione dei reati sopra illustrati, sono ritenuti idonei i principi di controllo e di comportamento individuati nel protocollo inerente al contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose.

Inoltre, per quanto concerne il reato di:

- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, si individua quale attività aziendale sensibile quella inerente alla gestione dei contenziosi e degli accordi transattivi;
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare, si individua quale attività aziendale sensibile quella inerente alla gestione del processo di selezione e assunzione del personale

²⁷ L'art. 25-duodecies è stato inserito nel D. Lgs. n. 231/2001 dall'art. 2 del D. Lgs. n. 109/2012, in vigore dal 9.8.2012.

²⁸ Deve sussistere una delle seguenti circostanze: a) impiego di più di tre lavoratori irregolari; b) impiego di lavoratori irregolari minori in età non lavorativa; c) esposizione a situazioni di grave pericolo.

Si rimanda pertanto ai protocolli previsti rispettivamente per il “Contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose”, per la “Gestione dei contenziosi e degli accordi transattivi” e per la “Gestione del processo di selezione e assunzione del personale” e per la “Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali”.

Detti protocolli si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.5 Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio.

7.5.1 Fattispecie di reato

Premessa

Il D.Lgs. 21.11.2007, n. 231 (di seguito Decreto antiriciclaggio) e il D.Lgs. 22.6.2007 n. 109, in attuazione di disposizioni comunitarie (Direttiva 2005/60/CE, c.d. “terza direttiva antiriciclaggio”) hanno profondamente riordinato la normativa in tema di prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di contrasto al finanziamento del terrorismo.

In data 10 marzo 2011, Banca d’Italia, d’intesa con la Consob e l’Isvap, in attuazione dell’art. 7 comma 2 del D.Lgs. n. 231/2007, ha emanato il “Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l’utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria ai fini di riciclaggio e di finanziamento del terrorismo”. Il Provvedimento si inserisce nel solco della crescente attenzione alle tematiche organizzative e di controllo interno che caratterizza la regolamentazione di vigilanza, nel presupposto che efficaci assetti organizzativi e di governo costituiscono condizione essenziale per prevenire e mitigare i fattori di rischio aziendali.

L’art. 25-octies del D.Lgs. n. 231/2001, introdotto dal Decreto antiriciclaggio, ha esteso la responsabilità dell’Ente ai reati di ricettazione, riciclaggio e impiego illecito anche per le ipotesi in cui non siano commessi con finalità di terrorismo o di eversione dell’ordine democratico, in ordine ai quali si rimanda all’*“Area sensibile concernente i reati con finalità di terrorismo o di eversione dell’ordine democratico, i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona”* o non presentino le caratteristiche di transnazionalità in precedenza previste²⁹. Da ultimo, l’art. 25-octies è stato modificato con l’introduzione del nuovo reato di autoriciclaggio³⁰.

Il rafforzamento della disciplina della responsabilità amministrativa degli Enti intende prevenire e reprimere più efficacemente il fenomeno dell’immissione nel circuito economico lecito di denaro, beni od utilità provenienti dalla commissione di delitti, in quanto di ostacolo all’amministrazione della

²⁹ Si ricorda che ai sensi dei commi 5 e 6 dell’art. 10 L. n. 146/2006, abrogati dal Decreto antiriciclaggio, il riciclaggio e l’impiego illecito costituivano reati presupposto della responsabilità degli Enti solo se ricorrevano le caratteristiche di transnazionalità previste dall’art. 3 della medesima legge.

³⁰ Il nuovo reato di autoriciclaggio è stato inserito nel codice penale e aggiunto ai reati presupposto del D.Lgs. n. 231/2001 dalla Legge n. 186/2014, entrata in vigore il 1.1.2015.

giustizia nelle attività di accertamento dei reati e di persecuzione dei colpevoli, oltre che, più in generale, lesiva dell'ordine economico, dell'integrità dei mercati e della libera concorrenza, in ragione degli indebiti vantaggi competitivi di cui godono gli operatori che dispongono di capitali di origine illecita.

Su un piano diverso, ma pur sempre finalizzate al contrasto del riciclaggio e del finanziamento del terrorismo, si collocano le previsioni contenute nel Decreto antiriciclaggio di specifici adempimenti posti a carico delle banche, degli intermediari finanziari e di altri determinati soggetti obbligati (adeguata verifica della clientela; registrazione e conservazione della documentazione delle operazioni; segnalazione di operazioni sospette; comunicazioni delle violazioni dei divieti in tema di denaro contante e dei titoli al portatore; comunicazione da parte degli Organi di controllo dell'Ente delle infrazioni riscontrate).

La violazione di detti obblighi di per sé non comporta la responsabilità amministrativa dell'Ente ai sensi del D.Lgs. n. 231/2001, non essendo detti illeciti ricompresi nell'elencazione dei cosiddetti reati presupposto ma è sanzionata ai sensi del Decreto antiriciclaggio, secondo una politica di tutela preventiva che prescinde dal ricorrere nelle concrete fattispecie di ipotesi di riciclaggio, ma che mira comunque ad assicurare il rispetto dei fondamentali principi della approfondita conoscenza della clientela e della tracciabilità delle transazioni, al fine di scongiurare anche il mero pericolo di inconsapevole coinvolgimento in attività illecite.

E' importante sottolineare che qualora l'addetto della Società contravvenisse a detti adempimenti nella consapevolezza della provenienza illecita dei beni oggetto delle operazioni, potrebbe essere chiamato a rispondere per i predetti reati, e potrebbe quindi conseguire anche la responsabilità amministrativa della SGR ai sensi del D.Lgs. n. 231/2001.

Si fornisce qui di seguito una sintetica descrizione degli elementi costitutivi dei reati in oggetto.

Ricettazione (art. 648 c.p.)

Commette il reato di ricettazione chiunque, allo scopo di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare. Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni di provenienza delittuosa.

E' inoltre richiesta la conoscenza della provenienza delittuosa del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi e

univoche - quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni - da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della provenienza illecita del denaro o del bene.

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

Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni od altre utilità provenienti da un delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

La norma va interpretata come volta a punire coloro che - consapevoli della provenienza delittuosa di denaro, beni o altre utilità - compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati.

Non è richiesto, ai fini del perfezionamento del reato, l'aver agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento. Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione.

Come per il reato di ricettazione, la consapevolezza dell'agente in ordine alla provenienza illecita può essere desunta da qualsiasi circostanza oggettiva grave e univoca.

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

La condotta criminosa si realizza attraverso l'impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio) c.p..

Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648-ter circoscrive la condotta all'impiego di tali risorse in attività economiche o finanziarie. Peraltro, in considerazione dell'ampiezza della formulazione della fattispecie del reato di riciclaggio, risulta difficile immaginare condotte di impiego di proventi illeciti che già non integrino di per sé il reato di cui all'art. 648-bis c.p..

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

Risponde del reato di autoriciclaggio chi, avendo commesso o concorso a commettere un qualsiasi delitto non colposo dal quale provengono denaro, beni o altre utilità, su tali proventi compie operazioni di impiego, sostituzione o trasferimento in attività economiche, finanziarie, imprenditoriali o speculative, con modalità tali da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

È esclusa la punibilità delle condotte consistenti nella destinazione dei proventi illeciti alla mera utilizzazione o godimento personale. È prevista un'aggravante di pena se il fatto è commesso nell'esercizio di attività professionale, economica o finanziaria e un'attenuante per il caso di ravvedimento operoso del reo.

Considerazioni comuni ai reati

Oggetto materiale

L'oggetto materiale dei reati può essere costituito da qualsiasi entità economicamente apprezzabile e possibile oggetto di scambio, quale il denaro, i titoli di credito, i mezzi di pagamento, i diritti di credito, i preziosi, i beni materiali e immateriali in genere. Deve però trattarsi di bene o utilità proveniente da delitto, vale a dire esso ne deve costituire il prodotto (risultato, frutto ottenuto dal colpevole con la commissione del reato), il profitto (lucro o vantaggio economico ricavato dal reato) o il prezzo (compenso dato per indurre, istigare, determinare taluno alla commissione del reato). Oltre che i delitti tipicamente orientati alla creazione di capitali illeciti (ad es.: concussione, corruzione, appropriazione indebita, truffa, reati fallimentari, traffico di armi o di stupefacenti, usura, frodi comunitarie, etc.) anche i reati in materia fiscale potrebbero generare proventi oggetto di riciclaggio o di autoriciclaggio, non solo nel caso di frodi (ad es. utilizzo di fatture per operazioni inesistenti che determinino un fittizio credito Iva da detrarre), ma anche nel caso in cui l'utilità economica conseguente al reato consista in un mero risparmio di imposta per mancato esborso di denaro proveniente da attività lecite (ad es. omessa o infedele dichiarazione di redditi, per importi oltre le soglie di rilevanza penale).

Condotta ed elemento soggettivo

Risponde dei reati di ricettazione, riciclaggio o reimpiego illecito, a seconda dei casi, il terzo estraneo al delitto che genera i proventi illeciti e che li riceve dal reo (o da altri, comunque conoscendone la provenienza illecita), per compiere su di essi le condotte previste dai reati medesimi.

Potrebbe invece rispondere a titolo di concorso nel delitto d'origine dei proventi illeciti e, di conseguenza, anche nel successivo reato di autoriciclaggio, qualora ne realizzi la condotta, il soggetto che avesse fornito un contributo causale di qualsiasi tipo, morale o materiale, alla commissione del reato d'origine, ad es. determinando o rafforzando il proposito criminoso del reo con la promessa, ancor prima della commissione del reato, del suo aiuto nel riciclare/impiegare i proventi.

Il reato di autoriciclaggio, diversamente da quanto previsto per i reati di riciclaggio e di impiego illecito, richiede che la condotta sia caratterizzata da modalità idonee a concretamente mascherare la vera provenienza delittuosa dei beni; l'interpretazione degli aspetti più innovativi della norma -

vale a dire il requisito del concreto ostacolo e la condizione di non punibilità dell'autoriciclatore ad uso personale (che sembrerebbe sempre da escludersi allorché il reato d'origine e il reimpiego avvengano nell'esercizio di un'attività d'impresa) – sarà necessariamente demandata alle applicazioni giurisprudenziali del nuovo reato.

Circa l'elemento soggettivo, come già accennato, i reati in esame devono essere caratterizzati dalla consapevolezza della provenienza delittuosa del bene. Secondo un'interpretazione particolarmente rigorosa, sarebbe sufficiente anche l'aver agito nel dubbio della provenienza illecita, accettandone il rischio (cosiddetto dolo indiretto od eventuale). Con riferimento all'operatività della SGR, va osservato che la presenza in determinate situazioni concrete di indizi di anomalia o di comportamenti anomali descritti nei provvedimenti e negli schemi emanati dalle competenti Autorità (per quanto concerne gli intermediari finanziari, dalla Banca d'Italia e dall'UIF) potrebbe essere ritenuta, accedendo alla particolarmente rigorosa interpretazione di cui sopra, come una circostanza oggettiva grave ed univoca atto a far sorgere il dubbio dell'illecita provenienza del bene.

Correlazioni col reato d'origine dei proventi illeciti

I reati della presente Area sensibile sussistono nelle ipotesi in cui le relative condotte siano successive al perfezionamento del reato che ha dato origine ai proventi illeciti, anche se compiute dopo la sua estinzione (ad es. per prescrizione o morte del reo), o anche se l'autore del medesimo non sia imputabile o punibile, oppure manchi una condizione di procedibilità (ad es., per difetto di querela, oppure di richiesta del Ministro della Giustizia, necessaria per perseguire i reati comuni commessi all'estero, ai sensi degli artt. 9 e 10 c.p.)³¹.

Per l'ipotizzabilità della responsabilità amministrativa dell'ente a titolo di autoriciclaggio, secondo alcune interpretazioni dottrinali, necessiterebbe che il dipendente o l'apicale abbia commesso nell'interesse o a vantaggio dell'ente non solo il reato di autoriciclaggio, ma anche il reato d'origine dei proventi illeciti e questo sia anch'esso espressamente previsto e punito dal D.Lgs. n. 231/2001 quale reato presupposto.

7.5.2 Attività aziendali sensibili

Il rischio che si verifichino nel contesto della SGR i reati di riciclaggio, intesi in senso lato (ivi compreso, quindi, l'autoriciclaggio), appare, invero, più marcato, quale rischio tipico del circuito finanziario, essenzialmente con riferimento ai rapporti con la clientela, e ad ipotesi di

³¹ In ordine all'irrelevanza dell'estinzione del reato che costituisce presupposto di un altro reato si veda l'art. 170, comma 1, c.p. ; per l'irrelevanza del difetto di una condizione di punibilità o procedibilità si veda l'art. 648, comma 3, c.p., richiamato anche dagli artt. 648-bis, 648-ter e 648-ter.1 c.p..

coinvolgimento/concorso in attività criminose della stessa; in particolare concerne l'instaurazione e la gestione dei rapporti continuativi con la clientela.

L'attività di prevenzione si basa sull'approfondita conoscenza della clientela e delle controparti e sull'osservanza degli adempimenti previsti dalla normativa in tema di contrasto al riciclaggio dei proventi di attività criminose e al finanziamento del terrorismo.

La centralità del rispetto rigoroso delle disposizioni dettate dal Decreto antiriciclaggio ai fini della prevenzione dei reati presupposto in questione discende anche dalle considerazioni che seguono. Va innanzitutto ricordato che il Decreto – ai fini dell'individuazione della tipologia delle condotte con le quali può concretarsi il riciclaggio, sottoposte all'obbligo di segnalazione delle operazioni sospette – all'art. 1 definisce "operazione" la trasmissione o la movimentazione di mezzi di pagamento" e all'art. 2 contiene un'elencazione di condotte, qualificate come di riciclaggio, di amplissima estensione, tale da comprendere comportamenti che, ai fini penali, potrebbero integrare la commissione del reato di autoriciclaggio, oppure la commissione degli altri reati presupposto in esame e che, se posti in essere da dipendenti o da soggetti apicali, potrebbero far sorgere la responsabilità amministrativa dell'ente stesso. Infine, l'elencazione in discorso è atta a ricomprendere anche condotte tipiche di altri reati, quali il favoreggiamento personale (art. 378 c.p.) che, se connotato dai requisiti della transnazionalità (al riguardo si rimanda al Capitolo 7.4), può costituire anch'esso reato presupposto della responsabilità amministrativa degli Enti.

Il rischio assume connotati diversi e appare meno rilevante con riferimento a quelle aree in cui la SGR, anche a prescindere dallo svolgimento delle attività tipiche, compie operazioni strumentali, acquista partecipazioni o movimenta il proprio patrimonio, assolve gli adempimenti contabili e fiscali. In tali ambiti difatti, sussiste una sviluppata articolazione dei presidi di controllo e delle procedure, già imposti dalla normativa di settore al fine di assicurare il rispetto di principi di trasparenza, correttezza, oggettività e tracciabilità della gestione.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose. Si evidenzia altresì che nell'ambito di protocolli che regolano altre attività sensibili - quali la *"Gestione dei contenziosi e degli accordi transattivi"*, la *"Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali"* e la *"Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni"* - sono previsti alcuni principi di controllo e di comportamento ispirati al medesimo criterio dell'attenta valutazione di fornitori, consulenti e controparti contrattuali in genere, principi che esplicano la loro efficacia preventiva anche in relazione ai reati sopra illustrati.

Più in generale, tutti i protocolli del presente Modello, laddove tesi a prevenire la commissione di reati che possono generare proventi illeciti, si devono intendere predisposti anche al fine della prevenzione dei reati di riciclaggio in senso lato. Si richiamano soprattutto i protocolli relativi alle Aree sensibili concernenti i reati societari - in particolare il protocollo sulla "*Gestione dell'informativa periodica*" - i reati e illeciti amministrativi riconducibili ad abusi di mercato, i reati informatici.

Tutti i sopra menzionati protocolli si completano con la normativa aziendale di dettaglio che regola le attività medesime e si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.5.2.1. Contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose

Premessa

Il presente protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di controllo e di comportamento per il contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose. Si intendono qui richiamate le disposizioni tempo per tempo vigenti in materia e in particolare le "Linee Guida per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi" della Capogruppo Intesa Sanpaolo, le "Regole in materia di Antiriciclaggio e Contrasto al Finanziamento del Terrorismo – Testo Unico Normativo" di Fideuram Investimenti SGR, nonché il Modello di organizzazione, gestione e controllo adottato nel gruppo FIDEURAM – Intesa Sanpaolo Private Banking per l'Antiriciclaggio e il contrasto al finanziamento del terrorismo.

Il presente protocollo si applica a tutte le Strutture coinvolte nelle attività sensibili sopra individuate nonché nelle attività di presidio dei rischi connessi alla normativa antiriciclaggio.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività, tracciabilità e riservatezza nell'esecuzione delle attività in oggetto.

Descrizione del processo

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

- identificazione e conoscenza della clientela e dei soggetti per conto dei quali i clienti operano, valutandone il profilo di rischio e cioè la probabilità di esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo tramite una apposita procedura di profilatura³².
La valutazione della sussistenza di tale rischio si basa sulla stessa conoscenza dei clienti e

³² Effettuata secondo le disposizioni previste dall'art. 20 del D.Lgs. n. 231/2007.

tiene conto, in particolare, di aspetti oggettivi (attività svolte dai clienti, le operazioni da essi compiute e degli strumenti utilizzati³³) e di aspetti soggettivi (soggetti sottoposti ad obblighi rafforzati di adeguata verifica; soggetti insediati in Paesi/centri caratterizzati da regimi fiscali o antiriciclaggio privilegiati quali quelli individuati dal GAFI come “non cooperativi”, etc.). Particolare attenzione deve essere posta nel rilevare il possibile coinvolgimento in operazioni o rapporti con soggetti (persone fisiche e giuridiche) censiti in liste pubbliche emanate in ambito nazionale e internazionale (liste ONU, UE, OFAC e liste MEF, ABI-UIF, di seguito tutte denominate per brevità “Black List”);

- apertura di nuovi rapporti continuativi e aggiornamento/revisione delle informazioni sui clienti esistenti, finalizzati al rispetto del principio della “*know your customer rule*”;
- monitoraggio dell’operatività e costante valutazione dei rischi di riciclaggio di denaro proveniente da attività illecite o di finanziamento del terrorismo, secondo tempistiche e modalità stabilite con riferimento al profilo di rischio assegnato;
- valutazione dell’operatività disposta dalla clientela riguardante soggetti/Paesi oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all’esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi);
- assolvimento degli obblighi normativi in materia di registrazione dei rapporti continuativi e delle operazioni disposte dalla clientela e conservazione delle relative informazioni;
- reporting esterno indirizzato alle Autorità di Vigilanza³⁴ e reporting interno ad esso finalizzate.

Le modalità operative per la gestione dei suddetti processi sono disciplinate nell’ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti. Tale normativa costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

³³ Ad esempio interposizione di soggetti terzi, impiego di strumenti societari, associativi o fiduciari suscettibili di limitare la trasparenza della proprietà e della gestione.

³⁴ Tali comunicazioni comprendono:

- invio all’UIF delle segnalazioni di operazioni sospette ai sensi degli artt. 41 e 42 del D.Lgs. n. 231/2007;
- invio all’UIF delle segnalazioni di blocco o congelamento dei fondi ai sensi del D.Lgs. n. 109/2007;
- invio all’Autorità di Vigilanza e al MEF delle comunicazioni ai sensi dell’art. 52 del D.Lgs. n. 231/2007.

- Livelli autorizzativi definiti:
 - la normativa interna individua i soggetti e le Strutture responsabili dell'attivazione/gestione/controllo dei processi sopra descritti.

- Segregazione dei compiti:
 - nelle situazioni individuate dalle disposizioni di legge e dalla normativa interna che impongono obblighi rafforzati di adeguata verifica della clientela (presenza di un rischio più elevato e altre ipotesi previste dall'art. 28 del Decreto antiriciclaggio), subordinazione dell'apertura di nuovi rapporti con clientela politicamente esposta (c.d. "PEP"), del mantenimento di rapporti preesistenti e dell'esecuzione delle operazioni al rilascio di una autorizzazione da parte di una Struttura diversa da quella operativa, che nello specifico è individuata nella Struttura Antiriciclaggio³⁵;
 - in relazione alle attività di monitoraggio dell'operatività volte ad individuare operazioni potenzialmente sospette, esistenza di una segregazione in base alla quale:
 - la competente struttura dell'outsourcer (sulla base di apposito contratto) estrae le operazioni potenzialmente sospette sia per le gestioni individuali che collettive, e le sottopone all'attenzione della Struttura Antiriciclaggio;
 - la Struttura Antiriciclaggio esamina le operazioni potenzialmente sospette, avvalendosi, qualora necessario, del supporto delle Strutture della SGR e/o della Banca, ovvero contattando il Private Banker tramite le stesse strutture della Banca;
 - nel caso in cui permanga un ragionevole sospetto, la Struttura Antiriciclaggio sottopone al Delegato di Gruppo (che coincide con il Responsabile Aziendale Antiriciclaggio e al quale è stata conferita la delega ex art. 42 D.Lgs. n. 231/2007 dal Consiglio di Amministrazione della Società) il relativo dossier;
 - il Delegato di Gruppo completa l'analisi dell'operazione potenzialmente sospetta, disponendo o meno l'inoltro della segnalazione alla competente Autorità.

³⁵ In data 5 maggio 2011, il Consiglio di Amministrazione di Fideuram Investimenti SGR S.p.A., in adempimento alle disposizioni previste dal "Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria ai fini di riciclaggio e di finanziamento del terrorismo" emanato da Banca d'Italia, ha:

- recepito il Modello di organizzazione, gestione e controllo di Gruppo in ambito Antiriciclaggio e Contrasto al finanziamento del terrorismo;
- approvato l'esternalizzazione della funzione Antiriciclaggio nella Controllante
- nominato il Referente Antiriciclaggio interno;
- conferito mandato all'Amministratore Delegato/Direttore Generale per lo svolgimento di tutte le attività necessarie e/o opportune per dare attuazione ai suddetti punti, ivi incluso il potere di formalizzare, quale Legale Rappresentante, il conferimento della delega di cui all'art. 42 del D.Lgs. 231/2007 al Delegato di Gruppo, ossia al Responsabile Aziendale Antiriciclaggio di., definendone la decorrenza.

- Attività di controllo: il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:
 - nell'ambito di una puntuale profilatura della clientela, verifica, all'atto dell'accensione del rapporto, per la clientela con profilo di rischio alto e medio-alto, da parte di ogni competente Struttura operativa, della correttezza e completezza dei dati censiti in anagrafe;
 - verifica, in occasione del censimento del cliente e periodicamente, dell'eventuale presenza del nominativo nelle versioni aggiornate delle specifiche "Black List";
 - monitoraggio nel medio-lungo periodo da parte delle Strutture operative preposte che garantisca con riguardo ai clienti nella fascia di rischio alto un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento (con particolare riguardo all'operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell'operazione, i fondi impiegati, l'orizzonte temporale dell'investimento, il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
 - monitoraggio e presidio da parte delle Strutture preposte al controllo interno della puntuale esecuzione nel pieno rispetto dei termini e delle disposizioni di legge e della normativa interna, delle attività delle Strutture operative in merito alla:
 - acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
 - valutazione delle operazioni rilevate dalle procedure informatiche in uso;
 - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
 - registrazione dei rapporti e delle operazioni in AUI e conservazione dei documenti e delle informazioni;
 - tutti i rapporti continuativi e le operazioni che comportano la trasmissione di mezzi di pagamento devono essere processati con modalità che consentano la registrazione procedurale nell'Archivio Unico Informatico con dati corretti e completi, anche avvalendosi di controlli automatici sulla qualità dei dati. A tale fine è indispensabile procedere alle attività di "integrazione" e "sistemazione" delle operazioni o dei rapporti in stato di "sospeso" entro i termini consentiti dalle procedure e comunque nei termini previsti dalla norma;
 - adozione di sistemi di controllo informatici atti ad impedire l'operatività riguardanti soggetti/Paesi oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti

all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi).

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto, in particolare:
 - conservazione riservata e ordinata, presso le Strutture di volta in volta interessate, di tutta la documentazione relativa alla identificazione e alla profilatura della clientela, in apposito archivio;
 - archiviazione sistematica di tutta la documentazione relativa all'operatività e ai controlli periodici effettuati sulle posizioni relative ai clienti, presso le strutture operative di competenza;
 - conservazione di traccia completa delle decisioni e delle motivazioni adottate sottostanti all'eventuale modifica del profilo del cliente e alla conseguente decisione circa l'inoltro o meno di una segnalazione di operazione sospetta.
- Riservatezza delle informazioni, con particolare riguardo a quelle relative all'individuazione dei titolari effettivi, alla profilatura dei clienti e ai processi di monitoraggio delle operazioni e di segnalazione delle operazioni sospette, mediante l'adozione di idonee misure informatiche e fisiche.
- Formazione: è prevista la sistematica erogazione di attività specificamente dedicate alla formazione continua dei dipendenti e dei collaboratori sui profili di rischio legati alla normativa antiriciclaggio e di contrasto al finanziamento del terrorismo.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nelle attività di contrasto del riciclaggio e del finanziamento del terrorismo, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare, le Strutture competenti sono tenute a:

- assicurare lo sviluppo e la gestione operativa delle applicazioni utilizzate nelle attività di contrasto finanziario al terrorismo/antiriciclaggio, e comunque in tutte le attività che si basano sulla “adeguata conoscenza della clientela”;
- verificare e garantire la diffusione all’interno delle strutture della SGR, rispettivamente, dei provvedimenti restrittivi - contenenti limitazioni operative in specifici settori - emanati da UE, OFAC - e delle “Black List” aggiornate, nonché l’adozione di procedure automatiche di rilevazione;
- garantire che l’operatività della clientela avvenga nel rispetto dei vincoli e delle autorizzazioni previsti dalle misure di embargo ovvero dalla disciplina relativa all’esportazione di determinate categorie di merci e/o materiali (es.: merce duale, sostanze chimiche pericolose);
- dettagliare nell’ambito di regolamenti/norme operative interne le regole comportamentali ad integrazione e maggiore specificazione della normativa esterna e dei principi sanciti dal presente protocollo;
- nel caso di valutazione di clientela ovvero di operazioni che interessino più strutture operative ovvero diverse società del Gruppo, collaborare tra loro e scambiare le informazioni finalizzate alla completa e adeguata conoscenza del cliente e delle sue abitudini operative;
- nei rapporti instaurati con corrispondenti estere, acquisire la documentazione con cui la società terza dichiara di adempiere agli obblighi antiriciclaggio e/o agli obblighi previsti da normative emanate da altri Stati (in particolare dagli Stati Uniti d’America);
- assicurare con continuità e sistematicità la formazione e l’addestramento del personale sulla normativa antiriciclaggio ed embarghi e sulle finalità dalla stesse perseguite;
- diffondere a tutti i collaboratori, indipendentemente dalle mansioni in concreto svolte, la normativa di riferimento e i relativi aggiornamenti.

Inoltre, i soggetti coinvolti, attenendosi a quanto prescritto nelle procedure aziendali, devono:

- all’atto dell’accensione di rapporti continuativi o del compimento di operazioni oltre la soglia di legge, anche se frazionate:
 - procedere all’identificazione della clientela e verificare l’eventuale presenza del nominativo nelle versioni aggiornate delle “Black List”;
 - verificare la sussistenza di eventuali titolari effettivi, acquisire informazioni sullo scopo e sulla natura del rapporto o dell’operazione e, qualora il cliente sia una società o un Ente, verificare la sussistenza dei poteri di rappresentanza e la struttura di proprietà e di controllo del cliente;

- procedere alla profilatura della clientela;
- mantenere aggiornati tutti i dati relativi ai rapporti continuativi al fine di consentire una costante valutazione del profilo economico e finanziario del cliente;
- effettuare l'adeguata verifica e la profilatura della clientela quando, indipendentemente da qualsiasi soglia di importo o di esenzione applicabile, vi sia il sospetto di riciclaggio o di finanziamento del terrorismo o sorgano dubbi sulla veridicità o sull'adeguatezza dei dati identificativi già acquisiti;
- mantenere l'assoluto riserbo sulle informazioni relative alla fascia di rischio antiriciclaggio attribuita al cliente e al relativo punteggio calcolato dalla procedura, che in nessun caso devono essere comunicati alla clientela;
- collaborare attivamente ai processi per la rilevazione e la segnalazione delle operazioni sospette;
- valutare se dare avvio all'iter di segnalazione in presenza di indici di anomalia anche se non rilevati dalle procedure informatiche o nei casi in cui risulti impossibile rispettare gli obblighi di adeguata verifica;
- verificare l'eventuale censimento dei clienti nelle versioni aggiornate delle Black List e bloccare o, comunque, non dare esecuzione ad operazioni che vedano coinvolti soggetti/Paesi oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi) o per le quali sussista comunque il sospetto di una relazione con il riciclaggio o con il finanziamento del terrorismo;
- rispettare rigorosamente le procedure interne in tema di registrazione dei rapporti e delle operazioni in AUI e di conservazione della documentazione.

I soggetti incaricati delle attività valutative o autorizzative previste dai processi in materia di antiriciclaggio, devono esercitare la discrezionalità loro rimessa secondo criteri di professionalità e ragionevolezza. In caso di conflitti di interesse, anche potenziali, di ordine personale o aziendale devono:

- informare immediatamente il proprio superiore gerarchico della sussistenza del conflitto di interessi precisandone la natura, i termini, l'origine e la portata;
- astenersi dall'attività valutativa/autorizzativa, rimettendo la decisione al proprio superiore gerarchico o alla Struttura specificamente individuata nella normativa interna per l'evenienza. A titolo esemplificativo, possono ricorrere situazioni di conflitto di interessi qualora l'interesse

personale interferisca (o appaia interferire) con l'interesse della Società o del Gruppo, impedendo l'adempimento obiettivo ed efficace delle proprie funzioni, ovvero in relazione al perseguimento di benefici personali impropri come conseguenza della posizione ricoperta in seno alla Società o al Gruppo.

E' inoltre fatto divieto comunicare, anche in modo involontario, a terzi (inclusi i soggetti con i quali sussistono rapporti di familiarità diretta o stretti legami propri o dei propri congiunti) per ragioni diverse da quelle di ufficio, il contenuto delle attività valutative/autorizzative al di fuori dei casi previsti dalla legge.

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

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

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.6 Area sensibile concernente i reati e illeciti amministrativi riconducibili ad abusi di mercato

7.6.1 Fattispecie di reato

Premessa

La Legge n. 62/2005 ha introdotto, agli articoli 184 e 185 del T.U.F. (D.Lgs. n. 58/1998), i reati di “abuso di informazioni privilegiate” e di “manipolazione di mercato”, oltre a due corrispondenti fattispecie di illecito amministrativo, disciplinate agli artt. 187-bis e 187-ter del T.U.F. medesimo.

La responsabilità amministrativa dell'Ente a fronte delle fattispecie penali di cui agli artt. 184 e 185 del T.U.F. è sancita dall'art. 25-sexies del D.Lgs. n. 231/2001. Si rammenta altresì che tra i reati societari che possono dar luogo alla responsabilità degli Enti vi è anche il reato di agiotaggio (vedi sopra paragrafo 7.3.1) riconducibile, al tempo stesso, alla materia degli abusi di mercato in senso lato riferiti, in particolare, agli strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato.

Per quanto invece concerne gli illeciti amministrativi di cui agli artt. 187-bis e 187-ter, la responsabilità dell'Ente discende dalla previsione contenuta nell'art. 187-quinquies del T.U.F., il quale rimanda ai medesimi principi, condizioni ed esenzioni del D.Lgs. n. 231/2001, ponendo però sempre a carico dell'Ente, a propria discolpa, la prova secondo cui l'autore dell'illecito ha agito esclusivamente nell'interesse proprio o di un terzo.

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

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

I maggiori rischi in relazione alla commissione degli illeciti si possono ipotizzare nei seguenti casi: di operazioni simulate, altri artifici o abuso di informazioni privilegiate per conto della SGR o a

favore di clienti della stessa ove sussista un interesse o vantaggio della SGR medesima, nonché diffusione di notizie false o fuorvianti, soprattutto in correlazione a operazioni effettuate sul mercato, prima o dopo tale diffusione.

In presenza di operazioni richieste dai clienti che facciano sospettare la commissione di uno degli illeciti di “Abuso di informazione privilegiata” o di “Manipolazione del mercato”, esiste (ai sensi dell’art. 187-nonies T.U.F.) un obbligo di segnalazione in capo all’intermediario: non può escludersi che, in astratto, si possa configurare un coinvolgimento della SGR nell’illecito commesso dal cliente in relazione alle concrete modalità di svolgimento delle attività da parte della SGR.

Si fornisce qui di seguito una descrizione delle fattispecie sopra indicate.

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

La fattispecie penale si realizza quando un soggetto acquista, vende o compie altre operazioni per conto proprio o di terzi su strumenti finanziari utilizzando informazioni privilegiate di cui sia venuto in possesso in ragione (i) della sua qualità di membro degli organi di amministrazione, direzione o controllo dell’emittente ovvero (ii) della partecipazione al capitale dell’emittente ovvero (iii) dell’esercizio di un’attività lavorativa, professionale ovvero di una funzione o di un ufficio. Può, inoltre, essere commesso da chi sia entrato in possesso di informazioni privilegiate in conseguenza della preparazione o commissione di un reato (es. intrusione in un sistema informatico ed estrazione di informazioni privilegiate).

La fattispecie si realizza altresì quando detti soggetti comunicano dette informazioni privilegiate al di fuori dell’esercizio del proprio lavoro o professione e anche quando raccomandano o inducono altri soggetti, sulla scorta delle informazioni privilegiate di cui sono in possesso, a compiere talune delle operazioni sopradescritte.

Per informazione privilegiata, ai sensi dell’art. 181, comma 1 del T.U.F. si intende quella “*di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari*”.

Nell’ambito dell’operatività della SGR, si riscontrano numerose fattispecie nelle quali possono profilarsi elementi di rischio, e che possono comportare la responsabilità della SGR nel caso in cui il reato sia commesso nell’interesse, esclusivo o concorrente, dell’Ente stesso (ad esempio, in relazione al fenomeno del *front running*³⁶).

³⁶ Modalità operativa con la quale si abusa dell’informazione privilegiata concernente gli ordini del cliente in attesa di esecuzione a vantaggio dello stesso intermediario ovvero a vantaggio di un altro cliente e anche nell’interesse o a vantaggio dello stesso intermediario.

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

La fattispecie penale si realizza quando qualcuno diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari indicati dall'art. 182 T.U.F. illustrato in premessa.

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

Come sopra illustrato, sono state introdotte specifiche sanzioni amministrative che sanzionano le medesime condotte materiali che formano oggetto delle fattispecie penali (artt. 184 e 185 T.U.F.): si precisa al riguardo che, mentre per l'illecito penale è necessario il dolo, per l'illecito amministrativo è sufficiente la colpa.

Va, in particolare, precisato che la condotta che integra l'illecito amministrativo di manipolazione del mercato ha una estensione più ampia rispetto alla fattispecie penale col medesimo nome, posto che il reato prevede la diffusione di notizie false o il compimento di operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, mentre l'illecito amministrativo contempla diverse condotte quali: la diffusione, tramite mezzi di informazione, compreso internet o ogni altro mezzo, di informazioni, voci o notizie false o fuorvianti, che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti; il compimento di operazioni idonee a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari ovvero a fissare in modo anomalo o artificioso il prezzo di tali strumenti ovvero che utilizzano artifici od ogni altro tipo di inganno o di espediente; altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

7.6.2 Attività aziendali sensibili

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

- Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato;
- Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato.

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

Detti protocolli si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.6.2.1. Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato

Premessa

Il presente protocollo si applica a tutti i componenti gli Organi Sociali e ai dipendenti della SGR che abbiano accesso ad informazioni privilegiate, nell'accezione di cui alla vigente normativa di legge e regolamentare, ovvero che gestiscano le comunicazioni della SGR al mercato e, in genere, all'esterno, intendendosi con tale espressione la distribuzione di ricerche e raccomandazioni nonché qualsiasi diffusione di notizie, dati o informazioni nell'ambito dei rapporti di business, delle attività di marketing o promozionali, dei rapporti con i mezzi di informazione, oltre che le comunicazioni di carattere obbligatorio c.d. price sensitive.

Il processo di gestione e di trattamento delle informazioni privilegiate potrebbe presentare potenzialmente occasioni per la commissione del reato di abuso di informazioni privilegiate ovvero della connessa fattispecie di illecito amministrativo, rispettivamente previsti dagli artt. 184 e 187-bis del T.U.F..

Una corretta gestione del processo in oggetto consente anche la prevenzione dei reati di agiotaggio e di manipolazione del mercato nonché dell'omologo illecito amministrativo - rispettivamente disciplinati dall'art. 2637 del codice civile e dagli artt. 185 e 187-ter del T.U.F. - relativamente alle condotte di cosiddetta "manipolazione informativa", presidiando il potenziale rischio di "diffusione di informazioni, voci o notizie false o fuorvianti".

Per quanto attiene la prevenzione delle condotte di cosiddetta "manipolazione operativa" si fa riferimento al protocollo per la "*Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato*".

Obiettivo delle regole sancite dal presente documento, in ottemperanza ai dettami della normativa vigente, è quello di garantire che:

- la circolazione delle informazioni nel contesto aziendale possa svolgersi senza pregiudizio del carattere privilegiato o confidenziale delle informazioni stesse ed evitare che dette informazioni siano condivise con soggetti non autorizzati nonché di assicurare che la divulgazione al mercato delle informazioni privilegiate avvenga in modo tempestivo, in forma completa e comunque in modo tale da evitare asimmetrie informative fra il pubblico;
- le informazioni privilegiate non vengano comunicate, anche in modo involontario, a terzi per ragioni diverse da quelle di ufficio, prescrivendo a tal fine ai componenti degli Organi Sociali ed ai dipendenti specifiche cautele comportamentali nonché, per i dipendenti, obblighi di

segnalazione alle competenti Strutture della SGR delle situazioni che possono comportare il rischio di una comunicazione non autorizzata di dette informazioni;

- i componenti gli Organi Sociali, i dipendenti ed i collaboratori non abusino delle informazioni privilegiate, di cui sono in possesso in virtù del ruolo ricoperto e/o delle funzioni svolte in ambito aziendale, per l'operatività in strumenti finanziari nell'interesse o per conto della SGR e/o a titolo personale;
- le comunicazioni della SGR al mercato e, in genere, all'esterno trovino adeguata disciplina e una precisa individuazione dei soggetti abilitati a effettuarle, affinché le stesse siano tali da evitare la divulgazione di informazioni o notizie false o fuorvianti, sia con riferimento alla SGR, sia con riferimento a società terze.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione e diffusione delle informazioni privilegiate di cui le strutture della SGR vengono a conoscenza è articolato sulla base delle specifiche responsabilità operative indicate nell'ambito della normativa di riferimento.

I criteri per l'individuazione delle informazioni privilegiate e le modalità operative per la gestione delle medesime sono disciplinati nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

In ragione dell'attività lavorativa e delle funzioni svolte nell'ambito dell'operatività aziendale, le Strutture della SGR possono trattare informazioni privilegiate aventi ad oggetto:

- la SGR stessa, la Capogruppo, la Controllante FIDEURAM – Intesa Sanpaolo Private Banking, le Società appartenenti al Gruppo Intesa Sanpaolo e gli strumenti finanziari emessi;
- le società clienti e gli strumenti finanziari da queste emessi;

- l'informazione trasmessa da un cliente e/o concernente gli ordini del cliente in attesa di esecuzione, che ha carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

L'informazione privilegiata può nascere da una decisione interna alla società (ad esempio le iniziative strategiche, gli accordi e le operazioni straordinarie) oppure derivare dall'accertamento di eventi o circostanze oggettive aventi un riflesso sull'attività dell'impresa e/o sul corso degli strumenti finanziari emessi (ad esempio situazioni contabili di periodo, notizie sul management) oppure derivare dalle attività svolte in nome o per conto di società terze o dalle attività svolte in conto proprio e conto terzi sui mercati finanziari.

Al fine di assicurare che la divulgazione al mercato delle informazioni price sensitive per il Gruppo, ossia che si riferiscano ad eventi che accadono nella sfera di attività della Capogruppo e/o delle Società dalla stessa controllate che abbiano effetti rilevanti sull'andamento economico-patrimoniale del Gruppo, avvenga nel rispetto della legge la Capogruppo ha elaborato una normativa di Gruppo che disciplina le seguenti fasi:

- individuazione delle informazioni privilegiate;
- predisposizione e approvazione del comunicato da diffondere al mercato;
- attestazione da parte del Dirigente Preposto, ai sensi dell'art. 154-bis del T.U.F., qualora le comunicazioni abbiano direttamente per oggetto informazioni economico – finanziarie consuntive della Capogruppo e del Gruppo;
- diffusione delle informazioni.

In relazione agli obblighi di correttezza e trasparenza nella divulgazione di notizie, dati e informazioni al fine di prevenire forme di manipolazione informativa, la SGR adotta specifiche procedure interne e di Gruppo volte a disciplinare tali aspetti.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- implementazione di sistemi di sicurezza logica e fisica e di altre procedure rispondenti alle migliori prassi, a garanzia della corretta gestione delle informazioni;
- adozione di misure di Gruppo per la separazione funzionale e logistica (c.d. Chinese Walls o Information Barriers) tra le Strutture organizzative che prestano servizi e attività di finanza

aziendale ai segmenti di clientela riferibili al c.d. lato Corporate e quelle che prestano servizi e attività di investimento o alcuni servizi accessori nei confronti degli investitori ovvero dei mercati finanziari riferibili al c.d. lato Market, affinché:

- le strutture del lato Market non vengano a conoscenza delle informazioni privilegiate o confidenziali conosciute dal lato Corporate;
- le strutture del lato Market non rispondano gerarchicamente alle strutture del lato Corporate né possano conoscerne le operazioni e attività, potendo così operare in modo indipendente e senza condizionamenti reciproci.

Considerato che la SGR è autorizzata alla prestazione dei soli servizi di investimento di gestione di portafogli e di consulenza in materia di investimenti nonché del servizio di gestione collettiva del risparmio (e pertanto appartenente al c.d. lato Market), i presidi di Gruppo in tema di separatezza funzionale e logistica, assicurano che i soggetti rilevanti della SGR coinvolti nella prestazione dei suddetti servizi non possano venire a conoscenza di informazioni privilegiate o di operazioni note a società del Gruppo che svolgono attività appartenenti al lato Corporate delle Chinese Walls;

- previsione dell'obbligo in capo ai dipendenti delle Strutture di business, di dare immediata notizia al proprio superiore gerarchico, che segnalerà la situazione alla Compliance, circa l'insorgere di situazioni di conflitto d'interessi (anche solo potenziale), per conto proprio o di terzi, derivante in particolare da rapporti di parentela o coniugio o da interessi economici patrimoniali propri o dei congiunti: ciò fermo restando l'obbligo generale di astensione previsto dall'art. 3 del Codice Interno di Comportamento di Gruppo;
- previsione di regole che individuano gli adempimenti ed i limiti cui sono soggetti, tra gli altri, i componenti gli Organi Sociali, i dipendenti ed i collaboratori quando vogliono effettuare operazioni di investimento su strumenti finanziari a titolo personale: dette regole prevedono, unitamente ai divieti generali applicabili a tutti i soggetti predetti, divieti e restrizioni specifiche per i dipendenti e collaboratori che operano in Strutture/Unità Organizzative nelle quali è maggiore la presenza di informazioni privilegiate, nonché obblighi di comunicazione, registrazione e monitoraggio delle operazioni personali consentite.

Il tutto come meglio individuato e disciplinato nelle policy e nei regolamenti interni e di Gruppo tempo per tempo vigenti che costituiscono parte integrante e sostanziale del presente protocollo.

Relativamente agli aspetti connessi alla diffusione al mercato dell'informazione privilegiata, il relativo iter procedurale è il seguente:

- qualora le informazioni price sensitive si riferiscano ad eventi che accadono nella sfera di attività della Società, il Presidente del Consiglio di Amministrazione, l'Amministratore Delegato e/o la Direzione Generale di Fideuram Investimenti SGR S.p.A. hanno la responsabilità dell'individuazione e della segnalazione delle circostanze e avvenimenti a tal fine rilevanti, con l'onere di contattare tempestivamente le strutture di Investor Relations e di Relazioni esterne della Capogruppo per il corretto adempimento degli obblighi di comunicazione al mercato;
- la Struttura di Investor Relations della Capogruppo predispone i comunicati stampa relativi ad informazioni price sensitive per il Gruppo, ossia che si riferiscano ad eventi che accadono nella sfera di attività della Capogruppo e/o delle Società Controllate che abbiano effetti rilevanti sull'andamento economico-patrimoniale del Gruppo, da inoltrare - previa autorizzazione degli organismi aziendali competenti e tramite la Struttura di Relazioni esterne della Capogruppo - alle Autorità di Vigilanza competenti in materia, via N.I.S., e alla stampa;
- la Struttura di Investor Relations della Capogruppo ha la responsabilità della gestione dei rapporti con gli analisti finanziari e gli investitori istituzionali al fine della divulgazione di informazioni rilevanti assicurandone l'omogeneità anche nelle ipotesi in cui la diffusione all'esterno avvenga tramite internet.

Principi di comportamento

Le Strutture, come pure i singoli dipendenti e collaboratori, a qualsiasi titolo coinvolte nelle attività di gestione e divulgazione delle informazioni privilegiate, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- è fatto obbligo di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la SGR, la Capogruppo, la Controllante FIDEURAM – Intesa Sanpaolo Private Banking o le altre Società del Gruppo e gli strumenti finanziari delle stesse, sia riguardanti Società terze in rapporto d'affari con la SGR e gli strumenti finanziari di queste ultime nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- è vietato compiere operazioni su strumenti finanziari della SGR, della Capogruppo, la Controllante FIDEURAM – Intesa Sanpaolo Private Banking o di Società del Gruppo e di Società terze in rapporto d'affari con la SGR stessa, in relazione alle quali si posseggano informazioni privilegiate circa l'emittente o il titolo stesso conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse. Tale divieto si applica a

qualsiasi tipo di operazione in strumenti finanziari (ad esempio: azioni, obbligazioni, warrant, covered warrant, opzioni, futures);

- è vietato compiere operazioni che anticipino le operazioni della clientela sugli stessi strumenti, considerandosi a tal fine informazione privilegiata anche l'informazione concernente gli ordini del cliente in attesa di esecuzione. Tale previsione implica anche il divieto di trasmettere a terzi informazioni sugli ordini o sulle informazioni ricevute dalla clientela;
- è possibile diffondere le informazioni privilegiate nell'ambito delle Strutture e uffici della SGR solo nei riguardi di coloro che abbiano effettiva necessità di conoscerle per motivi attinenti al normale esercizio del lavoro e nel rispetto delle misure di separazione previste, evidenziando la natura riservata delle informazioni;
- è vietato comunicare le medesime informazioni a terzi per ragioni diverse da quelle di ufficio (a titolo esemplificativo e non esaustivo: clienti, emittenti di titoli pubblicamente contrattati, ecc.) ovvero raccomandare o indurre terzi a compiere operazioni connesse alle informazioni privilegiate. Nel caso in cui gli eventuali soggetti terzi destinatari di tali informazioni non siano istituzionalmente tenuti ad un obbligo di riservatezza legale, regolamentare o statutario, è necessario formalizzare un accordo di *confidentiality* che imponga il reciproco dovere di riservatezza circa le informazioni scambiate;
- è vietato discutere informazioni privilegiate in luoghi pubblici o in locali in cui siano presenti estranei o comunque soggetti che non hanno necessità di conoscere tali informazioni. A titolo esemplificativo: si deve evitare di discutere tali informazioni in open space che ospitano strutture diverse, ascensori, corridoi, aree di ristoro, mense aziendali, ristoranti, treni, aerei, aeroporti, autobus e, in generale, in luoghi accessibili ad un pubblico indistinto; si deve porre particolare attenzione nell'uso di telefoni cellulari e di telefoni "viva voce";
- fatto salvo quanto previsto in materia di comunicazione al pubblico di informazioni privilegiate relative alla SGR, è vietato comunicare al mercato o ai media informazioni privilegiate relative alle società clienti della SGR. Qualora fosse richiesto un commento su specifiche operazioni relative a tali emittenti, ci si dovrà limitare a commentare i fatti già resi pubblici dall'emittente in base all'art. 114 del TUF; in ogni caso sono previsti obblighi di consultazione con le strutture aziendali che sono legittimamente in possesso delle informazioni privilegiate in modo che queste possano verificare che non siano anche involontariamente divulgate informazioni soggette a riservatezza;
- è vietato diffondere sia ad altro personale sia all'esterno della SGR, attraverso qualsiasi canale informativo, compreso internet, informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo

potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla SGR o al Gruppo e/o ai relativi strumenti finanziari nonché in relazione a Società terze in rapporto d'affari con la SGR o il Gruppo e ai relativi strumenti finanziari;

- è vietato produrre e diffondere studi e ricerche o altre comunicazioni di marketing in violazione delle norme, interne ed esterne, specificamente dettate per tale attività e, in particolare, senza garantire un'informazione chiara, corretta e non fuorviante e senza comunicare nei modi richiesti dalla normativa gli interessi rilevanti e/o i conflitti eventualmente sussistenti;
- è fatto obbligo, secondo quanto stabilito dalle norme interne in tema di sicurezza fisica e logica di custodire accuratamente documenti contenenti informazioni confidenziali e riservate, di assicurarsi che le proprie password rimangano segrete e che il proprio computer sia adeguatamente protetto attraverso il blocco temporaneo dello stesso nei momenti in cui ci si allontana dalla propria postazione. Si evidenzia inoltre che:
 - l'attività di produzione dei documenti (quali, ad esempio, stampa e fotocopiatura di documenti) contenenti informazioni privilegiate deve essere presidiata da personale a ciò abilitato;
 - i documenti in oggetto devono essere classificati come "confidenziali", "riservati" o, ove possibile, utilizzando nomi in codice per salvaguardare la natura dell'informazione in essi contenuta; l'accesso a informazioni confidenziali e riservate, quando elaborate/trattate/trasmesse/archivate in formato elettronico, deve essere regolato tramite inserimento di password o, per le Strutture che ne siano fornite, mediante l'apposito applicativo di crittografia;
 - i supporti recanti informazioni confidenziali e riservate devono essere custoditi in locali ad accesso fisico controllato, ovvero riposti in archivi custoditi o protetti al termine del loro utilizzo e non devono mai essere lasciati incustoditi, particolarmente quando portati all'esterno delle sedi di lavoro;
 - la distruzione dei supporti recanti informazioni confidenziali e riservate deve avvenire a cura degli stessi soggetti che ne dispongono, con le modalità più idonee ad evitare ogni improprio recupero del contenuto informativo.

Inoltre:

- con particolare riferimento all'attività di emissione di comunicati ufficiali al mercato, si precisa che essi devono essere redatti nel rispetto delle norme legali e regolamentari e, comunque, dei requisiti di correttezza, chiarezza, e parità di accesso all'informazione, dove:
 - per correttezza si intende un'informazione esaustiva e non fuorviante, in relazione alle legittime richieste di dati e notizie provenienti dal mercato;

- la chiarezza attiene alle forme con cui l'informazione è comunicata al mercato e ne comporta la completezza e l'intelligibilità in funzione dei diversi destinatari;
- per parità di accesso si intende l'inammissibilità di ogni forma di comunicazione selettiva di informazioni che possano avere rilevanza per la valutazione degli strumenti finanziari;
- con riferimento all'attività di divulgazione di informazioni privilegiate alle Autorità di Vigilanza, questa deve essere effettuata in modo completo, tempestivo e adeguato, nel rispetto delle norme e dei regolamenti in materia. Prima di tale comunicazione nessuna dichiarazione riguardante le informazioni privilegiate può essere rilasciata verso l'esterno.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.6.2.2 Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione delle operazioni di mercato su strumenti finanziari.

Il processo di gestione delle operazioni di mercato presenta potenzialmente occasioni per la commissione dei reati di agiotaggio e di manipolazione del mercato o del corrispondente illecito amministrativo previsti rispettivamente dall'art. 2637, dagli artt.185 e 187-ter del T.U.F., con riferimento alle condotte di c.d. "manipolazione operativa".

Per quanto attiene la prevenzione delle fattispecie – penale e amministrativa - della cosiddetta "manipolazione informativa" - che può consistere nella diffusione di informazioni, voci o notizie false o fuorvianti - si fa riferimento al protocollo per la *"Gestione e divulgazione delle informazioni ai fini della prevenzione degli illeciti penali e amministrativi in tema di Abusi di mercato"*, dove sono definiti i principi di controllo e di comportamento da osservare nel processo di gestione delle informazioni privilegiate di cui le Strutture operative della SGR potrebbero entrare in possesso in ragione dell'esecuzione dei compiti ad esse assegnati, ovvero in relazione alle comunicazioni della SGR al mercato e, in genere, all'esterno.

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

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione delle operazioni di mercato, ai fini del presente protocollo, riguarda da un lato l'investimento del patrimonio proprio della SGR, dall'altro le operazioni disposte dalla SGR per conto dei patrimoni gestiti (Fondi e Gestioni patrimoniali), concernente gli strumenti finanziari di cui all'art. 182 del T.U.F..

Con riferimento all'investimento del patrimonio proprio della SGR il processo ricomprende principalmente le seguenti attività:

- definizione della politica di investimento inerente all'utilizzo dei flussi di cassa per le attività di investimento in strumenti finanziari;
- definizione dell'operazione di investimento nel rispetto dei vincoli normativi e sulla base delle autorizzazioni ricevute e della politica di investimento dei flussi di cassa approvata dai competenti organi;
- preimputazione e trasmissione dell'ordine alla controparte per l'esecuzione;
- svolgimento degli adempimenti di carattere amministrativo/normativo connessi alla esecuzione dell'operazione.

Il processo di investimento relativo ai servizi prestati dalla SGR (gestione collettiva del risparmio, gestione di portafogli e consulenza in materia di investimenti) si suddivide in due fasi distinte:

- definizione della strategia di investimento;
- implementazione della strategia d'investimento, distinta per le:
 - gestioni collettive;
 - gestioni individuali.

Il processo di definizione della strategia di investimento è definito sulla base della *Risk Policy* dei singoli prodotti approvata dal Consiglio di Amministrazione in fase di avvio, eventualmente rivista periodicamente. Per i prodotti consulenzianti e gestiti in delega le indicazioni di *Risk Policy* sono ricevute dalle Società Clienti.

Con riferimento alle operazioni disposte per conto dei patrimoni gestiti (Fondi e Gestioni Patrimoniali), l'inoltro degli ordini agli intermediari, mediante l'apposito sistema, è effettuato

solamente dopo che gli stessi sono stati sottoposti al preventivo controllo positivo dei limiti (normativi, regolamentari e operativi).

La Società che fornisce il servizio di ricezione e trasmissione di ordini si attiva per la tempestiva trasmissione degli ordini ricevuti dalla SGR ai *broker* autorizzati dalla stessa, nel medesimo ordine con cui sono stati ricevuti e nel rispetto della *best execution*.

La SGR si avvale di un applicativo informatico per il monitoraggio quantitativo, la rilevazione e la segnalazione delle operazioni potenzialmente sospette, ai sensi della normativa “*Market Abuse Directive*”.

Le modalità operative per la gestione del processo sono disciplinate nell’ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti e in particolare approvazione da parte degli Organi competenti in base al vigente sistema dei poteri e delle deleghe:
 - della politica di investimento inerente l'utilizzo dei flussi di cassa per le attività di investimento in strumenti finanziari (patrimonio proprio della SGR);
 - della definizione della strategia di investimento per i patrimoni gestiti;
 - dei limiti operativi di investimento.
- Chiara e formalizzata assegnazione di poteri e responsabilità e esigenza di livelli autorizzativi definiti. In particolare, la politica di investimento del patrimonio proprio della SGR è approvata dal Consiglio di Amministrazione ed è rappresentata nella specifica normativa interna. Lo stesso vale per la strategia di investimenti dei patrimoni gestiti.
- Segregazione dei compiti attraverso una corretta allocazione delle responsabilità e separatezza organizzativa (funzionale e logistica) tra le Strutture che hanno a disposizione le informazioni privilegiate e quelle che operano sui mercati sulla base di informazioni di pubblico dominio o che intraprendono attività di gestione di investimenti.

- Attività di controllo sulle operazioni di compravendita titoli eseguite sui mercati attraverso un sistema di controlli differenziato che tenga conto delle diverse tipologie di strumenti finanziari trattati e della specificità del mercato di riferimento.
- Sottoposizione delle attività relative alla prestazione di servizi di investimento a monitoraggio da parte di Strutture di controllo di secondo livello della SGR, con particolare riferimento alla Compliance che svolge, per gli aspetti di competenza, un'attività di validazione preventiva e verifica costante dell'idoneità delle procedure interne in materia di prestazione dei servizi di investimento, anche sotto il profilo della conformità ai dettati normativi di riferimento avvalendosi altresì delle risultanze dell'Audit.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: in particolare, l'inoltro da parte dei gestori degli ordini di compravendita di strumenti finanziari agli intermediari è effettuato attraverso sistemi applicativi dedicati, nei quali sono mantenuti tutti i dettagli degli ordini inoltrati.
- Principi generali di gestione dell'operatività contenuti nella normativa interna di dettaglio che disciplina, in particolare:
 - aspetti fondamentali del processo di investimento;
 - regole per l'individuazione e la segnalazione delle operazioni sospette effettuate su iniziativa del gestore o su istruzioni impartite, per le GPM, direttamente dai Clienti (senza informare preventivamente il gestore/cliente dei controlli);
 - regole generali di comportamento, che richiedono alla Struttura competente di valutare caso per caso, prima dell'effettivo inoltro per l'esecuzione, le proposte di investimento dei flussi di cassa della SGR.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione del patrimonio proprio della SGR ovvero dei patrimoni gestiti dei clienti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare è fatto divieto di:

- porre in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari;

- compiere operazioni o ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- compiere operazioni o impartire ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;
- compiere operazioni od ordini di compravendita che utilizzano artifici od ogni altro tipo di inganno o di espediente;
- utilizzare altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

Si riportano di seguito le tipologie di “manipolazioni operative del mercato” vietate, previste dal “Codice di comportamento Assogestioni”.

1. Le “manipolazioni operative del mercato” possono consistere, a titolo esemplificativo e non esaustivo nelle fattispecie di seguito indicate.

(i) Operazioni dirette ad incrociare ordini sul titolo a prezzi anomali in modo da avvantaggiare la performance di un fondo/cliente a scapito di quella di un altro (improper matched orders)

La manipolazione si realizza, ad esempio, mediante l'incrocio di ordini di segno opposto per un elevato quantitativo in relazione al quantitativo medio scambiato e/o per un elevato numero di azioni (e/o mediante più incroci di ordini di segno opposto per quantitativi anche di minori dimensioni) ad un prezzo basso (alto) a beneficio (danno) del fondo che acquista (vende) e a danno di quello che vende (acquista).

(ii) Manipolazioni di titoli sottili detenuti in portafoglio, finalizzate a battere un benchmark prestabilito

Le manipolazioni consistono, ad esempio, nell'inserimento, nel portafoglio di un fondo/cliente caratterizzato da una gestione attiva (vale a dire finalizzata al conseguimento di performance superiori a quelle di un benchmark o parametro di riferimento prestabilito), di alcuni titoli sottili. Tali titoli sono poi manipolati con ordini o operazioni volti a farne aumentare i prezzi, in modo da consentire al fondo/cliente di ottenere performance superiori al benchmark o parametro di riferimento prestabilito.

- (iii) Manipolazioni dei titoli che hanno maggior peso nel portafoglio, dirette a far salire i prezzi dei titoli presenti nel portafoglio in modo da ottenere maggiori commissioni o remunerazioni**

Quando le commissioni spettanti alla società o le remunerazioni percepite dai gestori sono in funzione del valore del portafoglio del fondo/cliente, le manipolazioni in oggetto possono consistere nel far salire i prezzi dei titoli che hanno maggior peso nel portafoglio per ottenere commissioni o remunerazioni più elevate.

- (iv) Ordini di compravendita nonché esecuzione di operazioni prima o dopo che la società stessa o soggetti collegati alla medesima abbiano diffuso studi, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti**

La manipolazione si realizza, ad esempio, mediante la conclusione di accordi con intermediari appartenenti al medesimo gruppo della società o con i quali sono in essere rapporti commerciali (ad esempio, per i servizi di negoziazione) finalizzati a far aumentare (o diminuire) la valutazione o il “target price” in modo da consentire alla società di gestione, dopo che si produce l’effetto della valutazione sul prezzo del titolo, di poter in controtendenza vendere (o acquistare) a prezzi convenienti.

- (v) Occultamento della vera proprietà di uno strumento finanziario tramite la comunicazione, intenzionalmente fuorviante, al pubblico della proprietà di uno strumento finanziario a nome di altri soggetti collusi**

La manipolazione si realizza per mezzo dell’acquisizione, in accordo con altri soggetti (ad esempio, società del gruppo), di una partecipazione rilevante o di controllo in una società quotata, aggirando le norme relative alla comunicazione delle partecipazioni rilevanti.

- (vi) Aperture di posizioni comunicate al pubblico e immediatamente chiuse, salvo che le chiusure non siano determinate dalla richiesta di riscatti da parte della clientela**

La manipolazione consiste nella chiusura della posizione, effettuata sfruttando l’effetto positivo prodotto sui prezzi dai comunicati previsti dalla disciplina sulle partecipazioni rilevanti o da eventuali altre dichiarazioni diffuse spontaneamente.

2. Nel caso in cui la SGR gestisca fondi speculativi, flessibili, protetti o garantiti nonché fondi che hanno uno stile di gestione caratterizzato da un orizzonte d’investimento medio-breve, le

manipolazioni operative di mercato possono altresì consistere, sempre a titolo esemplificativo e non esaustivo, nelle fattispecie illustrate di seguito.

(i) Creazione di un trend o di bolle nei prezzi, realizzata, ad esempio, mediante il c.d. “pump and dump” o il c.d. “trash and cash”

Il c.d. “pump and dump” consiste nell’apertura di una posizione lunga su uno strumento finanziario seguita dall’effettuazione di ulteriori acquisti e/o nella diffusione di fuorvianti informazioni positive sullo strumento finanziario in modo da aumentarne il prezzo; gli altri partecipanti al mercato sono indotti ad effettuare altri acquisti dal risultante effetto sul prezzo e il manipolatore vende gli strumenti finanziari a prezzi più elevati.

Il c.d. “trash and cash” si realizza prendendo una posizione ribassista su uno strumento finanziario ed effettuando un’ulteriore attività di vendita e/o diffondendo fuorvianti informazioni negative sullo strumento finanziario in modo da ridurne il prezzo; il manipolatore chiude la posizione dopo la caduta del prezzo.

(ii) Compimento di operazioni in un mercato su uno strumento finanziario allo scopo di influenzare impropriamente il prezzo dello stesso strumento finanziario o di altri strumenti finanziari collegati negoziati sullo stesso o su altri mercati

La manipolazione si attua, in genere, in tre fasi: a) acquisizione di una posizione sullo strumento finanziario A ovvero esistenza di un interesse sullo strumento finanziario A già presente nel portafoglio gestito; b) manipolazione del prezzo dello strumento finanziario B, che determina o guida il valore dello strumento finanziario A; c) una volta che il prezzo di A si adegua al valore coerente con quello di B, chiusura della posizione su A, volontariamente o per effetto di regole già previste dal mercato o dal contratto (ad esempio, attraverso l’esercizio di opzioni).

3. Ove la SGR sia quotata o in rapporto di controllo (ovvero nel caso in cui l’emittente sia un fondo quotato), le manipolazioni operative potrebbero inoltre consistere, a titolo esemplificativo e non esaustivo nelle ipotesi delineate nel seguito.

(i) Costituzione di una soglia minima al corso dei prezzi (c.d. “creation of a floor in the price pattern”)

La manipolazione si realizza per mezzo della conclusione di operazioni o dell’inserimento di ordini in modo tale da evitare che i prezzi di mercato scendano al disotto di un certo

livello, ferma restando la possibilità di concludere operazioni rientranti nei programmi di acquisto di azioni proprie o nella stabilizzazione degli strumenti finanziari previsti dalla normativa (ovvero dal Regolamento 2273/2003 della Commissione europea o dalle prassi di mercato ammesse dall'autorità competente del mercato interessato). La strategia manipolativa potrebbe anche affiancarsi alla c.d. "creazione di trend" o ad un'operatività finalizzata ad innescare trend crescenti nei prezzi.

(ii) Occultamento della proprietà di uno strumento finanziario

In tal caso il comportamento coincide con quello che potrebbero attuare le SGR sui propri fondi, mutano gli strumenti finanziari che ne costituiscono oggetto. I presidi adottati dalla società coincidono, per modalità e tempi, con quelli già definiti per le SGR non quotate e ne differiscono, per l'oggetto.

Si evidenzia inoltre che, al fine di valutare se un comportamento sia idoneo a costituire manipolazione del mercato ai sensi dell'articolo 187-ter, comma 3, lettere a) e b) del D.Lgs. n. 58/98, sono da prendere in considerazione gli elementi e le circostanze di cui all'art. 43 co. 1 e 2 del Regolamento Mercati n. 16191 del 29.10.2007.

Si rileva, tuttavia, che gli elementi e le circostanze indicati nei commi 1 e 2 dell'art. 43 di cui sopra non sono da considerarsi esaustivi e non costituiscono di per sé necessariamente una manipolazione del mercato ai sensi dell'articolo 187-ter, comma 3, del D.Lgs. n. 58/98.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.7 Area sensibile concernente i reati in tema di salute e sicurezza sul lavoro

7.7.1 Fattispecie di reato

Premessa

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

Successivamente è stato emanato il c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro (D.Lgs. 9 aprile 2008 n. 81 come modificato dal D.Lgs. 3 agosto 2009 n. 106) che ha profondamente riordinato le molteplici fonti normative previgenti in materia. Per quanto concerne la responsabilità amministrativa degli Enti, l'art. 300 ha modificato l'art. 25-septies del D.Lgs. n. 231/2001 lasciando nella sostanza immutata l'individuazione delle fattispecie penali che costituiscono reati presupposto; l'art. 30 inoltre ha esplicitato le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.

Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro e alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.

Si fornisce qui di seguito una sintetica descrizione dei reati sopra menzionati.

Omicidio colposo (art. 589 c.p.)

Lesioni personali colpose gravi o gravissime (art. 590 comma 3 c.p.)

Le condotte punite dalle due fattispecie consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima.

Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

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

Vengono a tal proposito in considerazione molteplici disposizioni, ora in gran parte confluite nel Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro a seguito dell'abrogazione da parte del medesimo Testo Unico di varie leggi speciali previgenti, tra le quali, fondamentalmente: il D.P.R. 27.4.1955 n. 547 in tema di prevenzione degli infortuni; il D.P.R. 19.3.1956 n. 303 che disciplinava l'igiene del lavoro; il D.Lgs. 19.9.1994 n. 626 che conteneva norme generali sulla tutela della salute e della sicurezza dei lavoratori; il D.Lgs. 14.8.1996 n. 494 in tema di sicurezza dei cantieri.

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

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

7.7.2 Attività aziendali sensibili

La tutela della salute e della sicurezza sul lavoro è materia che pervade ogni ambito e attività aziendale.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di salute e sicurezza sul lavoro. Tale protocollo si completa con la normativa aziendale di dettaglio vigente in argomento.

Detto protocollo si applica anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.7.2.1. Gestione dei rischi in materia di salute e sicurezza sul lavoro

Premessa

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare e assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D.Lgs. n. 81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico, compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente e/o ai suoi delegati la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico, nonché compete ad entrambi, per gli ambiti di rispettiva pertinenza, il rispetto degli obblighi relativi all'affidamento di contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.

In ottemperanza a quanto disposto dalla predetta normativa, la SGR adotta e tiene aggiornato il "Documento di Valutazione dei Rischi", che contiene:

- la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori e il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione, del Rappresentante dei Lavoratori per la Sicurezza e del Medico Competente che hanno partecipato alla valutazione del rischio;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Tale Documento è redatto in conformità alla normativa nazionale e alle linee guida nazionali ed Europee (ISPESL, INAIL, UNI-EN-ISO, Agenzia Europea per la Salute e Sicurezza). In particolare sono recepite le "Linee Guida per un Sistema di Gestione della Salute e Sicurezza sul Lavoro (SGSL)" elaborate dall'UNI-INAIL nel settembre 2001. A tal fine il Documento di Valutazione del Rischio individua, entro l'organizzazione aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della propria politica di prevenzione nel rispetto delle norme di salute e sicurezza vigenti. Nel medesimo Documento vengono descritte le modalità specifiche con le quali

l'organizzazione risponde ai requisiti delle predette Linee Guida e sono esplicitati i processi operativi ed i documenti societari atti a garantire l'adempimento di quanto previsto dall'art. 30 – Modelli di organizzazione e di gestione – del D.Lgs. 81/2008.

La Società si è dotata, in relazione alla natura e dimensioni dell'organizzazione ed al tipo di attività svolta, di un'articolazione di funzioni/figure che assicura le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

Le Strutture/figure aziendali incaricate della gestione della documentazione inerente la materia, quali autorizzazioni/certificazioni/nullaosta rilasciati dalla Pubblica Amministrazione, sono tenute al rispetto dei principi di comportamento stabiliti e descritti nel protocollo *“Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione”*.

La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata e aggiornata a tutti i livelli organizzativi. Le linee d'azione generali della SGR devono essere orientate verso un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un “sistema di prevenzione e protezione”. Tutte le Strutture/figure della SGR devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti, compresi ristrutturazioni/allestimenti di siti operativi.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione dei rischi in materia di salute e sicurezza sul lavoro prevede le seguenti fasi:

- identificazione dei pericoli e loro classificazione (pericoli per la sicurezza e pericoli per la salute dei lavoratori);
- valutazione dei rischi;
- individuazione e predisposizione delle misure di prevenzione e di protezione;
- definizione di un piano di intervento con l'identificazione delle strutture/figure aziendali competenti all'attuazione di detti interventi;

- realizzazione degli interventi pianificati nell'ambito di un programma;
- verifica sull'attuazione e controllo sull'efficacia delle misure adottate.

Con specifico riferimento alla gestione dei cantieri temporanei e mobili (artt. 88 e seguenti del Testo Unico) che è nella responsabilità del "Committente", il processo prevede le seguenti fasi:

- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- designazione del Responsabile dei lavori e, ove necessario, del Direttore dei Lavori, del Coordinatore per la progettazione e del Coordinatore per l'esecuzione dei lavori, previa verifica dei requisiti professionali dei soggetti incaricati, e formalizzazione per iscritto dei relativi incarichi;
- pianificazione delle fasi di lavorazione e loro valutazione con particolare riferimento alle interazioni delle attività interferenti anche al contorno del cantiere ed alla eventuale compresenza di attività della Società e predisposizioni dei piani di sicurezza e coordinamento ovvero, ove non previsti dalla norma dei documenti di valutazione dei rischi interferenziali, anche per il tramite di professionisti incaricati;
- redazione delle lettere di richiesta di offerta con informativa alla controparte di quanto predisposto in tema di sicurezza (piani di sicurezza e coordinamento/documenti di valutazione dei rischi interferenziali);
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio/fornitura offerti nonché contenente dichiarazione di presa visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- esecuzione degli adempimenti tecnico-amministrativi, notifiche e comunicazioni alla pubblica amministrazione, anche per il tramite dei professionisti incaricati;
- aggiudicazione del servizio e stipula del contratto, con l'indicazione dei costi per la sicurezza e allegazione del piano di sicurezza e coordinamento/documento di valutazione dei rischi interferenziali;
- coordinamento nell'esecuzione delle attività fra le imprese/lavoratori autonomi e controlli sul rispetto delle misure nel cantiere, anche per il tramite dei professionisti incaricati.

Nei cantieri temporanei o mobili allestiti in unità operative ove sono presenti collaboratori della SGR i rischi derivanti da interferenze tra le due attività sono gestiti dal Committente, anche per il tramite di professionisti all'uopo incaricati, individuando le specifiche misure di prevenzione, protezione ed emergenza a tutela della salute e sicurezza dei collaboratori, dei clienti e delle imprese appaltatrici e lavoratori autonomi. Tali misure sono indicate nel Piano di Sicurezza e Coordinamento o, ove non

previsto, nel Documento unico di valutazione dei rischi interferenziali (in relazione al rispettivo campo di applicazione) elaborato a cura dei soggetti individuati dal Committente, che può avvalersi anche del supporto della Struttura di Prevenzione e Protezione del Datore di Lavoro della SGR.

Con specifico riferimento alla gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione rientranti nell'ambito di applicazione dell'art. 26 del Testo Unico, il processo prevede le seguenti fasi:

- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- informativa alla controparte circa i rischi specifici presenti nei luoghi in cui è chiamata ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla attività oggetto del contratto, nonché ove previsto dalla normativa, predisposizione del Documento di Valutazione dei Rischi Interferenziali (DUVRI), da inviare all'offerente ai fini della formulazione dell'offerta e parte integrante del contratto, contenente le misure idonee per eliminare o ridurre i rischi relativi alle interferenze delle attività connesse all'esecuzione del contratto e contestuale redazione della lettera di richiesta d'offerta ove prevista;
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio / fornitura offerti nonché contenente dichiarazione di presa di visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- aggiudicazione del servizio e stipula del contratto, con l'indicazione dei costi per la sicurezza e allegazione del DUVRI;
- esecuzione del servizio/fornitura da parte dell'aggiudicatario e cooperazione e coordinamento con le imprese/lavoratori autonomi, per gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, anche mediante reciproca informazione al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva e i rischi insiti nell'eventuale compresenza di personale, collaboratori e clienti della SGR;
- controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività.

Le modalità operative per la gestione del processo e l'individuazione delle Strutture/figure che hanno le responsabilità delle diverse fasi sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito del processo:
 - il sistema di gestione aziendale prevede la definizione di specifiche responsabilità e procedure al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato. In particolare, sono state individuate le figure aziendali che rivestono il ruolo rispettivamente di “Datore di Lavoro” e “Committente”. Tali figure possono impartire disposizioni in materia alle Strutture/figure aziendali, godono della più ampia autonomia organizzativa e dispongono dei più ampi poteri di spesa, anche con facoltà di delega e subdelega ai sensi dell'art. 16 comma 3 bis del Testo Unico;
 - è prevista un'articolazione di distinte funzioni/figure che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
 - tutti i soggetti/figure aziendali che intervengono nelle fasi del processo sopra descritto devono essere individuati e autorizzati con espressa previsione della normativa interna o tramite delega interna, da conferirsi e conservarsi a cura del Datore di Lavoro/Committente, ovvero a cura dei soggetti da costoro facoltizzati.

- Segregazione dei compiti tra i differenti soggetti/figure aziendali coinvolte nel processo di gestione dei rischi in materia di salute e sicurezza sul lavoro. In particolare:
 - le Strutture/figure operative che hanno il compito di realizzare e di gestire gli interventi (di natura immobiliare, informatica, di sicurezza fisica, ovvero attinenti a processi di lavoro e alla gestione del personale), sono distinte e separate dalla Struttura/figura alla quale, per legge e/o normativa interna, sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
 - le figure competenti designano i soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;
 - il Rappresentante dei Lavoratori per la Sicurezza collabora attivamente col Datore di Lavoro al fine di segnalare criticità e individuare le conseguenti soluzioni.

- Attività di controllo:
 - le Strutture/figure competenti devono attivare un piano aziendale di controllo sistematico al fine di verificare periodicamente la corretta applicazione/gestione nonché l'efficacia

delle procedure adottate e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro. Il piano, in particolare, deve contemplare:

- aree e attività aziendali da verificare (tra le quali le attività di natura organizzativa³⁷, di sorveglianza sanitaria, di informazione e formazione dei lavoratori, di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori);
- modalità di esecuzione delle verifiche, modalità di rendicontazione;

Il piano aziendale deve altresì assicurare:

- il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- l'acquisizione di documentazioni e certificazioni obbligatorie di legge (relative ad edifici, impianti persone, società ecc.) da parte delle competenti Strutture/figure;
- il rispetto del processo e degli adempimenti tecnici e amministrativi previsti dalle normative di legge.

Deve inoltre prevedere un idoneo sistema di controllo sulla sua efficace attuazione e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del piano devono essere adottati quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

- le Strutture/figure competenti devono controllare che tutte le misure di prevenzione e protezione programmate siano attuate, assicurando un costante monitoraggio delle situazioni di rischio e dell'avanzamento dei programmi di intervento previsti dagli specifici documenti di valutazione dei rischi. Tali Strutture/figure si avvalgono, laddove occorra, della collaborazione della Struttura deputata alla gestione delle risorse umane, nonché delle strutture di gestione e realizzazione di interventi immobiliari, di progettazione e gestione dei processi lavorativi, della sicurezza fisica, dei sistemi informativi, di gestione e manutenzione;
- il Rappresentante dei Lavoratori per la Sicurezza, nel rispetto delle norme di legge in materia, può accedere alla documentazione aziendale inerente la valutazione dei rischi e le misure di prevenzione relative e chiedere informazioni al riguardo. Il medesimo Rappresentante può accedere ai luoghi di lavoro e formulare osservazioni in occasione di visite e verifiche da parte delle Autorità competenti;

³⁷ Quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni del rappresentante dei lavoratori per la sicurezza

- tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente e il Responsabile del Servizio Prevenzione e Protezione visitano i luoghi di lavoro ove sono presenti lavoratori esposti a rischi specifici ed effettuano a campione sopralluoghi negli altri ambienti;
 - figure specialistiche di alta professionalità e con i titoli e i requisiti previsti dalle norme specifiche preventivamente valutate, contribuiscono alla valutazione e alla elaborazione di misure di tutela nel caso di rischi specifici (ad es. amianto, radon, elevato rischio di incendio) nonché nei cantieri temporanei e mobili (Responsabili dei lavori, Coordinatori per la Sicurezza, Progettisti, Direttori dei lavori ecc.);
 - le competenti Strutture/figure individuate dal Datore di Lavoro/Committente provvedono alla verifica dell'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare;
 - le competenti Strutture/figure individuate dal Committente verificano l'idoneità tecnico-professionale dei Responsabili dei Lavori e dei Coordinatori per la progettazione e per l'esecuzione, avute presenti anche le specifiche caratteristiche dei lavori oggetto di contratti di appalto;
 - qualora la documentazione prevista dal Testo Unico sia tenuta su supporto informatico, la competente Struttura verifica che le modalità di memorizzazioni dei dati e di accesso al sistema di gestione della predetta documentazione assicurino quanto previsto dall'art. 53 del Testo Unico;
 - il Datore di Lavoro e il Committente, ciascuno negli ambiti di competenza, vigilano ai sensi del comma 3 bis dell'art. 18 del Testo Unico in ordine all'adempimento degli obblighi in materia che la legge attribuisce a preposti, lavoratori, medici competenti, progettisti, fabbricanti, fornitori, installatori attraverso il piano aziendale di controllo sistematico sopra indicato;
 - con riferimento ai cantieri temporanei o mobili, il Committente verifica il corretto conferimento degli incarichi e l'adempimento degli obblighi posti a carico del Direttore dei Lavori, del Responsabile dei Lavori, del Coordinatore per la progettazione e del Coordinatore per l'esecuzione dei lavori, ove nominati; a tal fine acquisisce dagli stessi apposite relazioni periodiche che diano conto dell'attività svolta, delle eventuali criticità emerse e delle misure adottate per la loro soluzione.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - l'impiego di sistemi per la gestione informatica dei dati e delle documentazione prescritta dal Testo Unico deve avvenire nel rispetto dell'art. 53 del medesimo;

- ciascuna Struttura/figura di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, deve dotarsi di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività, ed è responsabile dell'archiviazione e della conservazione dei contratti stipulati nonché di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo;
- ciascuna Struttura/figura di volta in volta interessata è responsabile altresì dell'acquisizione, della conservazione e dell'archiviazione di documentazioni e certificazioni obbligatorie di legge, nonché della documentazione comprovante i requisiti tecnico-professionali delle imprese appaltatrici, dei lavoratori autonomi e dei soggetti destinatari di deleghe in materia di sicurezza (es.: Responsabile dei Lavori, Coordinatori per la progettazione e l'esecuzione).

Principi di comportamento

Le Strutture/figure, a qualsiasi titolo coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro, come pure tutti i dipendenti, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare, tutte le Strutture/figure sono tenute - nei rispettivi ambiti - a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela e valutando la scelta delle attrezzature di lavoro nonché la sistemazione dei luoghi di lavoro;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- astenersi dall'affidare incarichi a consulenti esterni eludendo criteri documentabili e obiettivi, quali professionalità qualificata e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, etc.) in occasione di accertamenti/procedimenti ispettivi;

- provvedere, nell'ambito dei contratti di appalto, d'opera o di fornitura, ad informare le controparti sui rischi specifici dell'ambiente in cui sono destinate ad operare e ad elaborare e applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese compresi gli eventuali lavoratori autonomi, evidenziando nei contratti per i quali sia prescritto i costi per la sicurezza;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure e attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nei confronti di tutti i lavoratori non dipendenti, con particolare riferimento all'ambito dei contratti regolati dal D.Lgs. n. 276/2003 e successive modifiche e integrazioni, nonché nei confronti dei soggetti beneficiari di iniziative di tirocinio e dei terzi in genere che dovessero trovarsi nei luoghi di lavoro;
- assicurarsi che, nell'impiego di sistemi di elaborazione automatica dei dati, le modalità di memorizzazione dei dati e di accesso al sistema di gestione della documentazione prescritta garantiscano quanto previsto dall'art. 53 del Testo Unico.

Parimenti, tutti i dipendenti sono tenuti a:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle Strutture/figure aziendali e dalle Autorità competenti;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, ogni situazione di pericolo potenziale o reale, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti (anche omissivi) che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. n. 231/2001.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.8 Area sensibile concernente i reati informatici

7.8.1 Fattispecie di reato

Premessa

La legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, stipulata a Budapest il 23.11.2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi.

La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D.Lgs. n. 231/2001 l'art. 24-bis, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli Enti.

La citata legge ha modificato anche il codice di procedura penale, essenzialmente al fine di agevolare e regolamentare le indagini e le operazioni di perquisizione e di sequestro dei dati informatici, imponendo all'Autorità procedente di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. E' stata altresì disposta l'integrazione dell'art. 132 del Codice della privacy (D.Lgs. n. 196/2003) che consente ora alle competenti Autorità di ordinare ai fornitori e agli operatori di servizi informatici o telematici di conservare per un periodo complessivamente non superiore a sei mesi i dati relativi al traffico telematico.

Non sono invece state recepite nell'ordinamento italiano le definizioni di "sistema informatico" e di "dato informatico" contenute nella Convenzione di Budapest; tali definizioni, che si riportano qui di seguito, potranno essere prese come riferimento dalla giurisprudenza in materia:

- "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;
- "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

Si illustrano qui di seguito i reati presupposto elencati dall'art. 24-bis del D.Lgs. n. 231/2001.

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

Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.

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

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

La condotta punita dall'art. 617-quater c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni.

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. spyware). L'impedimento od interruzione delle comunicazioni (c.d. "Denial of service") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fasulle.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro Ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema.

Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall'installazione non autorizzata di un software da parte di un dipendente.

L'art. 617-quinquies punisce il solo fatto della installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte a intercettare, impedire o interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

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

L'art. 635-bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.

Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.

L'art. 635-ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da Enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.

Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio.

Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615-ter c.p..

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

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

L'art. 635-quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati,

informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

L'art. 635-quinquies c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità.

In questa previsione, a differenza di quanto previsto all'art. 635-ter, non vi è più alcun riferimento all'utilizzo da parte di Enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato, sufficiente l'utilizzo da parte di Enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.

Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. E' da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento.

Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615-ter c.p..

Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

L'art. 615-quater punisce chiunque al fine di procurare a sé od ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo.

L'art. 615-quinquies punisce chiunque si procura, produce, riproduce importa, diffonde, comunica consegna o mette a disposizione di altri apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento.

Tali fattispecie perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche.

La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

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

L'art. 491-bis c.p. dispone che ai documenti informatici pubblici o privati aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità in scrittura privata, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche³⁸.

Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione.

³⁸ Si rammenta al riguardo che, ai sensi del Codice dell'amministrazione digitale (cfr. art. 1, lettera p) del D.Lgs. n. 82/2005), il documento informatico è "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ma:

- se non è sottoscritto con una firma elettronica (art. 1, lettera q), non può avere alcuna efficacia probatoria, ma può al limite, a discrezione del Giudice, soddisfare il requisito legale della forma scritta (art. 20, c. 1 bis);
- anche quando sia firmato con una firma elettronica "semplice" (cioè non qualificata) può non avere efficacia probatoria (il giudice dovrà infatti tener conto, per attribuire tale efficacia, delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento informatico);
- il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata ha l'efficacia prevista dall'articolo 2702 del codice civile (al pari della scrittura privata), fa cioè piena prova, fino a querela di falso, se colui contro il quale è prodotto ne riconosce la sottoscrizione

Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.).

Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

Tra i reati richiamati dall'art. 491-bis, sono punibili a querela della persona offesa la falsità in scrittura privata (art. 485 c.p.) e, se riguardano una scrittura privata, l'uso di atto falso (art. 489 c.p.) e la soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

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

Tale reato è commesso dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato³⁹. Il soggetto attivo del reato può essere evidentemente soltanto un soggetto "certificatore qualificato", che esercita particolari funzioni di certificazione per la firma elettronica qualificata.

A tale specifico proposito si osserva che la SGR non riveste la qualifica di "certificatore qualificato" e che quindi tale disposizione non è di immediato interesse per la stessa.

* * *

Più in generale può osservarsi che molte fattispecie di reati informatici in concreto potrebbero non presentare il requisito della commissione nell'interesse o a vantaggio della SGR, indispensabile affinché possa conseguire la responsabilità amministrativa della stessa. Per altro verso si ricorda che qualora fossero integrati tutti gli elementi previsti dal D.Lgs. n. 231/2001 la responsabilità della SGR potrebbe sorgere, secondo la previsione contenuta nell'art. 8 del Decreto, anche quando l'autore del reato non sia identificabile (dovrebbe quantomeno essere provata la provenienza della condotta da un soggetto apicale o da un dipendente, anche se non identificato), evenienza tutt'altro che improbabile nel campo della criminalità informatica, in ragione della complessità dei mezzi impiegati e dell'evanescenza del cyberspazio, che rendono assai difficile anche l'individuazione del luogo ove il reato stesso possa ritenersi consumato.

³⁹ Per certificato qualificato si intende, ai sensi dell'art. 1 lettere e) ed f) del D. Lgs. n. 82/2005, l'attestato elettronico che collega all'identità del titolare i dati utilizzati per verificare le firme elettroniche, che sia conforme ai requisiti stabiliti dall'allegato I della direttiva 1999/93/CE, rilasciato da certificatori - vale a dire i soggetti che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi con quest'ultime - che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

Va infine ricordato che anche l'art. 640-ter c.p., che punisce il delitto di frode informatica perpetrata ai danni dello Stato o di altro Ente pubblico, costituisce reato presupposto della responsabilità amministrativa degli Enti; al riguardo si rimanda al Capitolo 7.2.1.

7.8.2 Attività aziendali sensibili

Le attività della SGR nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.

La SGR ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni di Vigilanza e al Codice della privacy, per prevenire e controllare i rischi in tema di tecnologia dell'informazione (IT), a tutela del proprio patrimonio informativo e dei dati personali della clientela e dei terzi.

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i comportamenti illeciti come sopra descritti è la:

- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo.

Si riporta di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili a detta attività e che si completa con la normativa aziendale di dettaglio che regola l'attività medesima.

Detto protocollo si applica anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.8.2.1. Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione e nell'utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo.

In particolare, si applica a:

- tutte le Strutture coinvolte nella gestione e l'utilizzo dei sistemi informativi che si interconnettono/utilizzano *software* della Pubblica Amministrazione ovvero delle Autorità di Vigilanza;
- tutte le Strutture deputate alla progettazione, alla realizzazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni;
- tutte le Strutture che hanno la responsabilità di realizzare interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del Patrimonio Informativo di Gruppo nelle attività connesse con il proprio mandato e nelle relazioni con i terzi che accedono al Patrimonio Informativo del Gruppo;
- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi della SGR e trattano i dati del Patrimonio Informativo di Gruppo.

Ai sensi del D.Lgs. n. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione dei delitti informatici contemplati dall'art. 24-bis, nonché del reato di frode informatica ai danni dello Stato o di altro Ente pubblico previsto dall'art. 640-ter del codice penale e richiamato dall'art. 24 del Decreto. Inoltre, mediante l'accesso alle reti informatiche potrebbero essere integrate le condotte illecite aventi a oggetto le opere dell'ingegno protette⁴⁰.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

⁴⁰ Per la descrizione delle relative condotte si veda l' "Area sensibile concernente i reati contro l'industria ed il commercio ed i reati in materia di violazione del diritto d'autore".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della SGR, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

L'utilizzo e la gestione di sistemi informatici e del Patrimonio Informativo sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi della SGR.

Tra i sistemi informativi utilizzati dalla SGR vi sono altresì hardware e software per l'espletamento di adempimenti verso la Pubblica Amministrazione che prevedano il ricorso a specifici programmi forniti dagli stessi Enti, ovvero la connessione diretta con gli stessi.

Si rendono quindi necessarie una efficace e stringente definizione di norme e misure di sicurezza organizzative, comportamentali e tecnologiche e la realizzazione di attività di controllo, peculiari del presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo in coerenza con la normativa vigente.

Alla luce delle considerazioni che precedono, di seguito si declinano i processi sui quali si basa il presidio posto in essere sulla gestione e sull'utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo della SGR.

Il processo di gestione della sicurezza informatica si articola nelle seguenti fasi:

- analisi del rischio IT e definizione dei requisiti di sicurezza informatica;
- gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;
- gestione normativa e architettura di sicurezza informatica;
- monitoraggio eventi sicurezza informatica e gestione crisi di sicurezza informazioni;
- progettazione e realizzazione soluzioni di sicurezza informatica.

Il processo di prevenzione frodi si articola nelle seguenti fasi:

- identificazione delle misure atte al rafforzamento della prevenzione;
- monitoraggio dell'evoluzione delle frodi informatiche, anche per quanto riguarda eventuali aspetti di sicurezza fisica correlati;
- presidio delle attività necessarie all'intercettazione e alla soluzione delle minacce verso gli asset aziendali;
- gestione delle comunicazioni con le Forze dell'Ordine.

Il processo di gestione della sicurezza fisica si articola nelle seguenti fasi:

- gestione protezione di aree e locali ove si svolge l'attività;
- gestione sicurezza fisica dei sistemi periferici (ambienti di filiali, sede centrale, altre reti).

Il processo relativo alla progettazione, sviluppo e attivazione dei servizi ICT si articola nelle seguenti fasi:

- progettazione, realizzazione e gestione delle soluzioni applicative e delle infrastrutture tecnologiche di Gruppo;

Il processo di gestione e supporto ICT si articola nelle seguenti fasi:

- erogazione dei servizi ICT;
- monitoraggio del funzionamento dei servizi ICT e gestione delle anomalie;
- assistenza agli utenti attraverso attività di Help desk e problem solving.

Le modalità operative per la gestione dei processi descritti sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

Fatti salvi i requisiti di sicurezza propri del software della Pubblica Amministrazione o delle Autorità di Vigilanza utilizzato dalla SGR, il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica dei processi sopra descritti. In particolare:
 - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso" in ragione delle funzioni svolte all'interno della SGR;
 - le variazioni al contenuto dei profili sono eseguite dalle Strutture della SGR deputate al presidio della sicurezza logica, su richiesta delle Strutture interessate. La Struttura richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte;
 - ogni utente ha associato un solo profilo abilitativo in relazione al proprio ruolo aziendale nel rispetto del principio del minimo privilegio. In caso di trasferimento o di modifica dell'attività dell'utente, viene attribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato;

- Segregazione dei compiti:
 - sono assegnati distinti ruoli e responsabilità di gestione della sicurezza delle informazioni; in particolare:
 - sono attribuite precise responsabilità in modo che siano presidiati gli ambiti di indirizzo e governo della sicurezza, di progettazione, di implementazione, di esercizio e di controllo delle contromisure adottate per la tutela del Patrimonio Informativo aziendale;
 - sono attribuite precise responsabilità per la gestione degli aspetti di sicurezza alle strutture che sviluppano e gestiscono sistemi informativi;
 - sono definite le responsabilità e i meccanismi atti a garantire la gestione di eventi di sicurezza anomali e delle situazioni di emergenza e crisi;
 - sono attribuite precise responsabilità della predisposizione, validazione, emanazione e aggiornamento delle norme di sicurezza a strutture distinte da quelle incaricate della gestione;
 - le attività di implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del software sono organizzativamente demandate a strutture differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi;
 - sono attribuite precise responsabilità per garantire che il processo di sviluppo e manutenzione delle applicazioni, effettuato internamente o presso terzi, sia gestito in modo controllato e verificabile attraverso un opportuno iter autorizzativo.

- Attività di controllo: le attività di gestione e utilizzo dei sistemi informativi della SGR e del Patrimonio Informativo di Gruppo sono soggette ad una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza. Le attività di controllo costituiscono valido presidio anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate.

I controlli previsti, declinati dalle relative policy interne, si basano sulla definizione di specifiche attività finalizzate alla gestione nel tempo anche degli aspetti inerenti alla protezione del Patrimonio Informativo del Gruppo, quali:

- la definizione degli obiettivi e delle strategie di sicurezza;
- la definizione di una metodologia di analisi dei rischi ai quali è soggetto il patrimonio informativo da applicare a processi e asset aziendali, stimando la criticità delle informazioni in relazione ai criteri di riservatezza, integrità e disponibilità;
- l'individuazione delle contromisure adeguate, con riferimento ai livelli di rischio rilevati, verificando e controllando il corretto mantenimento dei livelli di sicurezza stabiliti;
- l'adeguata formazione del personale sugli aspetti di sicurezza per sviluppare una maggiore sensibilità;
- la predisposizione e l'aggiornamento delle norme di sicurezza, al fine di garantirne nel tempo l'applicabilità, l'adeguatezza e l'efficacia;
- i controlli sulla corretta applicazione e il rispetto della normativa definita.

Le principali attività di controllo, tempo per tempo effettuate, e specificamente dettagliate nella normativa interna di riferimento, sono le seguenti:

Con riferimento alla sicurezza fisica:

- protezione e controllo delle aree fisiche (perimetri/zone riservate) in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi.

Con riferimento alla sicurezza logica:

- identificazione e autenticazione dei codici identificativi degli utenti;
- autorizzazione relativa agli accessi alle informazioni richiesti;
- previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse.

Con riferimento all'esercizio e alla gestione di applicazioni, sistemi e reti:

- previsione di una separazione degli ambienti (sviluppo, collaudo e produzione) nei quali i sistemi e le applicazioni sono installati, gestiti e mantenuti in modo tale da garantire nel tempo la loro integrità e disponibilità;
- predisposizione e protezione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionale ad un corretto e sicuro svolgimento delle attività;

- previsione di misure per le applicazioni in produzione in termini di installazione, gestione dell'esercizio e delle emergenze, protezione del codice, che assicurino il mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni trattate;
- attuazione di interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti;
- pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema;
- gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità tramite la regolamentazione e il controllo sull'utilizzo degli strumenti, delle apparecchiature e di ogni asset informativo in dotazione nonché mediante la definizione di modalità di custodia, riutilizzo, riproduzione, distruzione e trasporto fisico dei supporti rimovibili di memorizzazione delle informazioni, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati;
- monitoraggio di applicazioni e sistemi, tramite la definizione di efficaci criteri di raccolta e di analisi dei dati relativi, al fine di consentire l'individuazione e la prevenzione di azioni non conformi;
- prevenzione da software dannoso tramite sia opportuni strumenti e infrastrutture adeguate (tra cui i sistemi antivirus) sia l'individuazione di responsabilità e procedure per le fasi di installazione, verifica di nuovi rilasci, aggiornamenti e modalità di intervento nel caso si riscontrasse la presenza di software potenzialmente dannoso;
- formalizzazione di responsabilità, processi, strumenti e modalità per lo scambio delle informazioni tramite posta elettronica e siti web;
- adozione di opportune contromisure per rendere sicura la rete di telecomunicazione e gli apparati a supporto e garantire la corretta e sicura circolazione delle informazioni;
- previsione di specifiche procedure per le fasi di progettazione, sviluppo e cambiamento dei sistemi e delle reti, definendo i criteri di accettazione delle soluzioni;
- previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali.

Con riferimento allo sviluppo e alla manutenzione delle applicazioni:

- individuazione di opportune contromisure e adeguati controlli per la protezione delle informazioni gestite dalle applicazioni, che soddisfino i requisiti di riservatezza, integrità

e disponibilità delle informazioni trattate, in funzione degli ambiti e delle modalità di utilizzo, dell'integrazione con i sistemi esistenti e del rispetto delle disposizioni di Legge e della normativa interna;

- previsione di adeguati controlli di sicurezza nel processo di sviluppo delle applicazioni, al fine di garantirne il corretto funzionamento anche con riferimento agli accessi alle sole persone autorizzate, mediante strumenti, esterni all'applicazione, per l'identificazione, l'autenticazione e l'autorizzazione.

Con riferimento alla gestione degli incidenti di sicurezza:

- previsione di opportuni canali e modalità di comunicazione per la tempestiva segnalazione di incidenti e situazioni sospette al fine di minimizzare il danno generato e prevenire il ripetersi di comportamenti inadeguati e attivare l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
 - tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali, risultano tracciate attraverso sistematica registrazione (sistema di log files);
 - tutti i transiti in ingresso e in uscita degli accessi alle zone riservate, del solo personale che ne abbia effettiva necessità previa debita autorizzazione, sono rilevati tramite appositi meccanismi di tracciatura;
 - è prevista la tracciatura delle attività effettuate sui dati, compatibili con le leggi vigenti al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del Patrimonio Informativo di Gruppo sono tenute ad osservare le modalità esposte nel presente

protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- le Strutture coinvolte nei processi devono predisporre e mantenere il censimento degli applicativi che si interconnettono con la Pubblica Amministrazione o con le Autorità di Vigilanza e/o dei loro specifici software in uso;
- i soggetti coinvolti nel processo devono essere appositamente incaricati;
- ogni dipendente/amministratore del sistema è tenuto alla segnalazione all'Alta Direzione aziendale di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente e attivando l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la SGR dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del Patrimonio Informativo di Gruppo nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- 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 del Gruppo, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad 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 ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre, o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti 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;

- riprodurre banche di dati su supporti non contrassegnati dalla SIAE, diffonderle in qualsiasi forma senza l'autorizzazione del titolare del diritto d'autore o in violazione del divieto imposto dal costitutore;
- rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;
- importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.9 Area sensibile concernente i reati contro l'industria e il commercio e i reati in materia di violazione del diritto d'autore

7.9.1 Fattispecie di reato

Premessa

La L. 23.7.2009 n. 99 - Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in tema di energia - in un più ampio quadro di iniziative di rilancio dell'economia e di tutela del "Made in Italy", dei consumatori e della concorrenza, ha attratto nell'ambito della responsabilità da reato degli Enti numerose norme penali, alcune delle quali dalla stessa legge emanate o riformulate. In particolare, nel testo novellato del D.Lgs. n. 231/2001, gli artt. 25-bis e 25-bis.1 richiamano fattispecie previste dal codice penale in tema di industria e di commercio⁴¹, mentre l'art. 25-novies - al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno⁴² e i gravi danni economici arrecati agli autori e all'industria connessa – rimanda a reati contemplati dalla legge sul diritto d'autore (L. n. 633/1941).

Si descrivono qui di seguito gli illeciti in questione.

Contraffazione, alterazione o uso di marchi o di segni distintivi ovvero di brevetti, modelli e disegni di prodotti industriali (art. 473 c.p.)

La norma punisce le condotte di chi, pur potendo accertare l'altrui appartenenza di marchi e di altri segni distintivi di prodotti industriali, ne compie la contraffazione, o altera gli originali, ovvero fa uso dei marchi falsi senza aver partecipato alla falsificazione⁴³.

Integrano la contraffazione le ipotesi consistenti nella riproduzione identica o nell'imitazione degli elementi essenziali del segno identificativo, in modo tale che ad una prima percezione possa

⁴¹ A seguito della modifica apportata dalla L. n. 99/2009, l'art. 25-bis del D. Lgs. n. 231/2001 - che in precedenza riguardava i soli ai reati di falsità in materia di monete e di valori di bollo - concerne anche i delitti previsti dagli articoli 473 e 474 c.p., i quali hanno in comune con i primi il bene giuridico principalmente tutelato e cioè la fede pubblica, intesa quale affidamento che la generalità dei cittadini ripone nella veridicità di determinati oggetti, segni o attestazioni.

⁴² Ai sensi dell'art. 1 della L. n. 633/1941 sono tutelate le opere dell'ingegno di carattere creativo che appartengono alla letteratura (anche scientifica o didattica), alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì protetti come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

⁴³ Per "fare uso" dei marchi falsi dovrebbero intendersi condotte residuali, quali ad esempio l'apposizione su propri prodotti di marchi falsificati da terzi. Si deve trattare cioè di condotte diverse sia dalla messa in circolazione di prodotti recanti marchi falsi previste nell'art. 474 c.p., sia dalle condotte più propriamente realizzative della contraffazione, quale ad esempio la riproduzione del marchio altrui nelle comunicazioni pubblicitarie, nella corrispondenza commerciale, nei siti internet, ecc..

apparire autentico. Si tratta di quelle falsificazioni materiali idonee a ledere la pubblica fiducia circa la provenienza di prodotti o servizi dall'impresa che è titolare, licenziataria o cessionaria del marchio registrato. Secondo la giurisprudenza è tutelato anche il marchio non ancora registrato, per il quale sia già stata presentata la relativa domanda, in quanto essa lo rende formalmente conoscibile. E' richiesto il dolo, che potrebbe sussistere anche qualora il soggetto agente, pur non essendo certo dell'esistenza di altrui registrazioni (o domande di registrazione), possa dubitarne e ciononostante non proceda a verifiche.

Il secondo comma sanziona le condotte di contraffazione, nonché di uso da parte di chi non ha partecipato alla falsificazione, di brevetti, disegni e modelli industriali altrui⁴⁴. Anche questa disposizione intende contrastare i falsi materiali che, nella fattispecie, potrebbero colpire i documenti comprovanti la concessione dei brevetti o le registrazioni dei modelli. La violazione dei diritti di esclusivo sfruttamento economico del brevetto è invece sanzionata dall'art. 517-ter c.p..

Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

L'art. 474 c.p. punisce le condotte di coloro che, estranei ai reati di cui all'art. 473 c.p., introducono in Italia prodotti industriali recanti marchi o segni distintivi contraffatti o alterati, oppure detengono per la vendita, mettono in vendita o comunque in circolazione prodotti contraffatti, sempre che non siano già punibili per l'introduzione in Italia. E' sempre richiesto il fine di trarre profitto.

Il detentore potrebbe essere punito, oltre che per il reato in questione, anche a titolo di ricettazione, qualora fosse a conoscenza fin dal momento dell'acquisto della falsità dei segni distintivi apposti ai prodotti dal suo fornitore o da altri. Si ricorda che, ai sensi dell'art. 25-octies del Decreto, anche il reato di ricettazione può dar luogo alla responsabilità amministrativa degli Enti.

Turbata libertà dell'industria e del commercio (art. 513 c.p.)

Il reato, perseguibile a querela, consiste nel compiere atti di violenza sulle cose o nell'utilizzare mezzi fraudolenti al fine di ostacolare od impedire il regolare svolgimento di un'attività commerciale od industriale, sempre che non siano integrati reati più gravi (ad es. incendio, oppure uno dei reati informatici previsti dall'art. 24-bis del Decreto). Ad esempio, si è ritenuto sussistere il reato nel caso di inserimento nel codice sorgente del proprio sito internet - in modo da renderlo maggiormente visibile ai motori di ricerca - di parole chiave riferibili all'impresa o ai prodotti del concorrente, al fine di dirottare i suoi potenziali clienti.

⁴⁴ Il Codice della proprietà industriale (D.Lgs. n. 30/2005), all'art. 2 recita: "La brevettazione e la registrazione danno luogo ai titoli di proprietà industriale. Sono oggetto di brevettazione le invenzioni, i modelli di utilità, le nuove varietà vegetali. Sono oggetto di registrazione i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori."

Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)

Commette questo delitto l'imprenditore che compie atti di concorrenza con violenza o minaccia. La norma, introdotta nel codice penale dalla legge antimafia "Rognoni – La Torre" n. 646/1982, trova applicazione anche al di fuori della criminalità mafiosa e intende contrastare gli atti diretti a impedire o limitare l'intervento sul mercato di operatori concorrenti. Il reato sussiste anche quando la violenza o la minaccia sia posta in essere da terzi per conto dell'imprenditore, oppure non sia direttamente rivolta al concorrente, ma ai suoi potenziali clienti. Potrebbe ad esempio ravvisarsi il reato nelle ipotesi di: minaccia di arrecare un danno ingiusto diretta ai partecipanti a una gara pubblica al fine di conoscere le loro offerte e formularne più basse minaccia, nel rapporto con un proprio cliente, di applicare condizioni peggiorative, ovvero, nel rapporto con un proprio fornitore, di non effettuare altri ordini nel caso in cui il fornitore ricorra ai servizi di/fornisca un determinato concorrente.

Frodi contro le industrie nazionali (art. 514 c.p.)

Il delitto incrimina chiunque cagioni un danno contro l'industria nazionale, ponendo in circolazione od in commercio prodotti industriali con marchi o segni distintivi contraffatti. Le dimensioni del danno devono essere tali da colpire non singole imprese, ma l'economia industriale italiana.

Frode nell'esercizio del commercio (art. 515 c.p.)

L'illecito, sempre che non sussistano gli estremi della truffa, consiste nella consegna all'acquirente da parte di chi esercita un'attività commerciale di una cosa mobile per un'altra, o che, pur essendo della stessa specie, per origine, provenienza, qualità o quantità, sia diversa da quella pattuita.

Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

Il reato è commesso di chi pone in vendita o in commercio sostanze alimentari non genuine, vale a dire sostanze, cibi e bevande che, pur non pericolosi per la salute, siano stati alterati con aggiunta o sottrazione di elementi, od abbiano composizione diversa da quella prescritta.

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

Il delitto consiste nel mettere in vendita o comunque in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi⁴⁵ atti ad indurre in inganno il compratore sull'origine,

⁴⁵ L'art. 181-bis, comma 8, della L. n. 633/1941 dispone che ai fini della legge penale il contrassegno SIAE è considerato segno distintivo di opera dell'ingegno.

provenienza o qualità dell'opera o del prodotto. E' sufficiente che i segni distintivi, anche in relazione alle altre circostanze del caso concreto (prezzi dei prodotti, loro caratteristiche, modalità della vendita) possano ingenerare nel comune consumatore confusione con i prodotti affini (ma diversi per origine, provenienza o qualità) contrassegnati dal marchio genuino. La norma tutela l'onestà nel commercio e si applica sussidiariamente, quando non ricorrano gli estremi delle più gravi incriminazioni degli artt. 473 e 474 c.p.. In essa ricadono casi quali la contraffazione e l'utilizzo di marchi non registrati, l'uso di recipienti o di confezioni con marchi originali, ma contenenti prodotti diversi, l'uso da parte del legittimo titolare del proprio marchio per contraddistinguere prodotti con standard qualitativi diversi da quelli originariamente contrassegnati dal marchio (il caso non ricorre se la produzione sia commissionata ad altra azienda, ma il committente controlli il rispetto delle proprie specifiche qualitative).

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)

Il reato consta di due diverse fattispecie. La prima, perseguibile a querela, punisce chiunque, potendo conoscere dell'esistenza di brevetti o di registrazioni altrui, fabbrica o utilizza ai fini della produzione industriale oggetti o altri beni, usurpando un titolo di proprietà industriale o in violazione dello stesso. Qualora sussista la falsificazione dei marchi o un'altra delle condotte previste dagli artt. 473 e 474 c.p., l'usurpatore potrebbe rispondere anche di tali reati.

La seconda fattispecie concerne la condotta di chi, al fine di trarne profitto, introduce in Italia, detiene per la vendita, pone in vendita o mette comunque in circolazione beni fabbricati in violazione dei titoli di proprietà industriale. Se le merci sono contraddistinte da segni falsificati si applica anche l'art. 474, comma 2, c.p..

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

Le condotte punite consistono nell'apportare a prodotti agroalimentari false o alterate indicazioni geografiche o denominazioni d'origine⁴⁶ nonché, ai fini di trarne profitto, nell'introdurre in Italia, detenere per la vendita, porre in vendita o mettere comunque in circolazione i medesimi prodotti con indicazioni o denominazioni contraffatte.

⁴⁶ Ai sensi dell'art. 29 del D. Lgs. n. 30/2005 sono protette: *“le indicazioni geografiche e le denominazioni di origine che identificano un paese, una regione o una località, quando siano adottate per designare un prodotto che ne è originario e le cui qualità, reputazione o caratteristiche sono dovute esclusivamente o essenzialmente all'ambiente geografico d'origine, comprensivo dei fattori naturali, umani e di tradizione”*.

Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941)**Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941)**

Commette il primo delitto in esame chiunque, senza averne il diritto, a qualsiasi scopo e in qualsiasi forma, mette a disposizione del pubblico un'opera dell'ingegno protetta o parte di essa, immettendola in un sistema di reti telematiche mediante connessioni di qualsiasi genere. In alcuni particolari casi - per finalità culturali o di libera espressione e informazione e con determinate limitazioni - è consentita la comunicazione al pubblico di opere altrui⁴⁷.

Il secondo delitto in oggetto consiste nell'abusivo utilizzo dell'opera dell'ingegno altrui (mediante riproduzione, trascrizione, diffusione in qualsiasi forma, commercializzazione, immissione in reti telematiche, rappresentazione o esecuzione in pubblico, elaborazioni creative, quali le traduzioni, i compendi, ecc.) aggravato dalla lesione dei diritti morali dell'autore. Alla condotta di per sé già abusiva deve cioè aggiungersi anche la violazione del divieto di pubblicazione imposto dall'autore, o l'usurpazione della paternità dell'opera (c.d. plagio), ovvero la sua deformazione, mutilazione, o altra modificazione che offenda l'onore o la reputazione dell'autore.

Entrambe le incriminazioni si applicano in via residuale, quando non risulti presente il dolo specifico del fine di trarre un profitto od un lucro, che deve invece caratterizzare le condotte, in parte identiche, più severamente sanzionate dagli artt. 171-bis e 171-ter.

Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941)

Il primo comma della norma, con riferimento ai programmi per elaboratore⁴⁸, punisce le condotte di abusiva duplicazione, nonché di importazione, distribuzione, vendita, detenzione a scopo commerciale od imprenditoriale (quindi anche per uso limitato all'ambito della propria impresa), concessione in locazione, quando hanno per oggetto programmi contenuti in supporti privi del contrassegno della Società italiana degli autori ed editori (SIAE). Costituiscono inoltre reato l'approntamento, la detenzione o il traffico di qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione da utilizzi abusivi dei programmi.

⁴⁷ Si veda ad es. l'art. 65 della L. n. 633/1941, secondo il quale gli articoli di attualità pubblicati nelle riviste e nei giornali possono essere utilizzati da terzi, se la riproduzione non è stata espressamente riservata, purché si indichino la fonte, la data e l'autore.

⁴⁸ Ai sensi dell'art. 2, n. 8, della L. n. 633/1941 sono tutelati i programmi per elaboratore in qualsiasi forma espressi purché originali, quale risultato di creazione intellettuale dell'autore. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso. Gli artt. 64-bis, 64-ter e 64-quater della citata legge disciplinano l'estensione dei diritti che competono all'autore del programma e i casi di libera utilizzazione dello stesso, vale a dire le ipotesi in cui sono consentite riproduzioni od interventi sul programma anche senza specifica autorizzazione del titolare dei diritti.

Il secondo comma, con riferimento alla tutela dei diritti dell'autore di una banca di dati⁴⁹, punisce la riproduzione - permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma - su supporti non contrassegnati dalla SIAE, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o la dimostrazione in pubblico non autorizzate dal titolare del diritto d'autore. Sono altresì sanzionate le condotte di estrazione e di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati, in violazione del divieto imposto dal costitutore⁵⁰ della medesima banca dati. Per estrazione deve intendersi il trasferimento di dati permanente o temporaneo su un altro supporto con qualsiasi mezzo o in qualsivoglia forma e per reimpiego qualsivoglia forma di messa a disposizione del pubblico dei dati mediante distribuzione di copie, noleggio, trasmissione con qualsiasi mezzo e in qualsiasi forma. Tutte le predette condotte devono essere caratterizzate dal dolo specifico del fine di trarne profitto, vale a dire di conseguire un vantaggio, che può consistere anche solo in un risparmio di spesa.

Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941)

La norma elenca una nutrita casistica di condotte illecite - se commesse per uso non personale e col fine di lucro - aventi ad oggetto: opere destinate al circuito televisivo, cinematografico, della vendita o del noleggio; supporti di qualunque tipo contenenti opere musicali, cinematografiche, audiovisive, loro fonogrammi, videogrammi o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche, didattiche, musicali, multimediali. Sono, infatti, punite:

- le condotte di abusiva integrale o parziale duplicazione, riproduzione, diffusione in pubblico con qualsiasi procedimento;
- le condotte, poste in essere da chi non ha partecipato all'abusiva duplicazione o riproduzione, di introduzione in Italia, detenzione per la vendita o distribuzione, messa in commercio, cessione a qualsiasi titolo, proiezione in pubblico o trasmissione televisiva o radiofonica, far ascoltare in pubblico le duplicazioni o riproduzioni abusive;

⁴⁹ Ai sensi dell'art. 2, n. 9, della L. n. 633/1941, le banche di dati consistono in raccolte di opere, dati od altri elementi indipendenti, sistematicamente o metodicamente disposti e individualmente accessibili mediante mezzi elettronici od in altro modo. Resta ovviamente salva la distinta tutela riconosciuta ai diritti d'autore eventualmente esistenti sulle opere dell'ingegno inserite nella banca dati. Gli artt. 64-quinquies e 64-sexies della legge disciplinano l'estensione dei diritti dell'autore della banca di dati nonché i casi di libera utilizzazione della stessa.

⁵⁰ I diritti del costitutore sono regolati dagli artt. 102-bis e 102-ter della L. n. 633/1941. Per costitutore si intende colui che effettua investimenti rilevanti per la creazione, la verifica o la presentazione di una banca di dati e al quale compete, indipendentemente dalla tutela che spetta al suo autore in ordine ai criteri creativi secondo i quali il materiale è stato scelto e organizzato, il diritto di vietare le operazioni di estrazione o di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati. Per le banche di dati messe a disposizione del pubblico, ad esempio mediante libero accesso on line, gli utenti, anche senza espressa autorizzazione del costitutore, possono effettuare estrazioni o reimpieghi di parti non sostanziali, valutate in termini qualitativi e quantitativi, per qualsivoglia fine, salvo che l'estrazione od il reimpiego siano stati espressamente vietati o limitati dal costitutore.

- le medesime condotte elencate al punto che precede (salvo l'introduzione in Italia e il far ascoltare in pubblico) riferite a supporti di qualunque tipo, anche se non frutto di abusiva duplicazione o riproduzione, privi del prescritto contrassegno SIAE o con contrassegno falso.

Sono altresì sanzionate le condotte abusive concernenti, in sintesi: la diffusione di servizi ricevuti con decodificatori di trasmissioni criptate; i traffici di dispositivi che consentano l'accesso abusivo a detti servizi o di prodotti diretti ad eludere le misure tecnologiche di contrasto agli utilizzi abusivi delle opere protette; la rimozione o l'alterazione delle informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti, ovvero l'importazione o la messa in circolazione di opere dalle quali siano state rimosse od alterate le predette informazioni.

Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941)

Commettono il reato i produttori od importatori di supporti contenenti software destinati al commercio che omettono di comunicare alla SIAE i dati necessari all'identificazione dei supporti per i quali vogliono avvalersi dell'esenzione dall'obbligo di apposizione del contrassegno SIAE⁵¹.

E' altresì punita la falsa attestazione di assolvimento degli obblighi di legge rilasciata alla SIAE per l'ottenimento dei contrassegni da apporre ai supporti contenenti software od opere audiovisive.

Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941)

Il delitto è commesso da chiunque, per fini fraudolenti produce, importa, promuove, installa, pone in vendita, modifica o utilizza anche per solo uso personale, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

7.9.2 Attività aziendali sensibili

Con riferimento all'operatività della SGR, i rischi di commissione dei reati contro l'industria e il commercio e in materia di violazione del diritto d'autore più verosimilmente possono presentarsi:

- nei rapporti con la clientela, con riguardo alla prestazione di servizi a favore di soggetti coinvolti nelle attività illecite in questione;

⁵¹ L'art. 181-bis, comma 3, della L. n. 633/1941 dispone che, fermo restando il rispetto dei diritti tutelati dalla legge, possono essere privi del contrassegno SIAE i supporti contenenti software da utilizzarsi esclusivamente tramite elaboratore elettronico, che non contengano opere audiovisive intere non realizzate espressamente per il programma per elaboratore, ovvero riproduzioni di parti eccedenti il 50% di preesistenti opere audiovisive, che diano luogo a concorrenza nell'utilizzazione economica delle stesse.

- nella partecipazione a gare pubbliche, con particolare riferimento a comportamenti illeciti nei confronti dei partecipanti;
- nell'approvvigionamento o nell'utilizzo di prodotti, software, banche dati e altre opere dell'ingegno, strumentali all'attività della SGR o destinati ad omaggi per la clientela.

Meno rilevante appare il rischio con riferimento alle attività di ideazione e di lancio di nuovi prodotti, di gestione del naming e dei marchi della Società, della comunicazione esterna o pubblicitaria e delle iniziative di marketing, nonché con riferimento alle attività di gestione dei rapporti con la clientela, nell'ottica della lealtà della concorrenza e della correttezza e trasparenza delle pratiche commerciali, e ciò in ragione della sviluppata articolazione dei presidi di controllo e delle procedure già imposti dalla normativa di settore.

Si rimanda pertanto ai seguenti protocolli:

- "Stipula dei rapporti contrattuali con la Pubblica Amministrazione";
- "Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali";
- "Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni";
- "Contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose";
- "Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo";

che contengono processi, principi di controllo e principi di comportamento diretti a prevenire anche la commissione dei reati di cui al presente Capitolo.

Detti protocolli si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.10 Area sensibile concernente i reati ambientali

7.10.1 Fattispecie di reato

Premessa

L'art. 25-undecies del D.Lgs. n. 231/2001 individua gli illeciti dai quali, nella materia della tutela penale dell'ambiente, fondata su disposizioni di matrice comunitaria, discende la responsabilità amministrativa degli enti⁵².

Si tratta di reati descritti nel codice penale, nel D.Lgs. n. 152/2006 (Codice dell'ambiente, per brevità nel seguito C. A.) e in varie leggi speciali, sia di natura delittuosa, sia di tipo contravvenzionale⁵³. Le fattispecie sono le seguenti.

Inquinamento ambientale (art. 452-bis c.p.)

La norma punisce chi cagiona abusivamente una compromissione o un deterioramento significativi e misurabili delle acque, dell'aria, del suolo o del sottosuolo, di un ecosistema o della biodiversità.

Disastro ambientale (art. 452-quater c.p.)

La norma punisce chi abusivamente provoca un disastro ambientale, che consiste nell'alterazione dell'equilibrio di un ecosistema che sia irreversibile, o la cui eliminazione sia particolarmente onerosa ed eccezionale, oppure nell'offesa all'incolumità pubblica, in ragione della gravità del fatto, per estensione, o per gli effetti, o per il numero di persone offese o esposte a pericolo.

Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)

Sono punite molteplici condotte abusive (cessione, acquisto, ricezione, trasporto, importazione, esportazione, detenzione, abbandono, ecc.) concernenti materiali ad alta radioattività.

Associazione a delinquere con aggravante ambientale (art. 452-octies c.p.)

⁵² L'art. 25-undecies del D.Lgs. n. 231/01, in vigore dal 16 agosto 2011, nel testo dapprima inserito dal D.Lgs. n. 121/11, emanato in recepimento delle Direttive 2008/99/CE e 2009/123/CE, e successivamente modificato dalla L. n. 68/15, in vigore dal 29 maggio 2015, che ha introdotto nel codice penale i nuovi delitti contro l'ambiente.

⁵³ Le fattispecie delittuose sono quelle previste dal codice penale (eccetto gli artt. 727-bis e 733-bis) e dal C.A. agli artt. 258, comma 4, 2° periodo, 260, c. 1 e 2, 260-bis, commi 6, 7 e 8, nonché i reati di falsi documentali in tema di commercio di specie animali e vegetali e il reato di inquinamento doloso provocato da navi. Di regola, le fattispecie contravvenzionali sono punite anche se commesse a titolo di colpa; i delitti di inquinamento e disastro ambientale, se commessi per colpa, sono puniti ai sensi dell'art. 452-quinquies codice penale e costituiscono anch'essi reati presupposto della responsabilità amministrativa degli enti.

La norma prevede una specifica aggravante di pena per i reati di associazione a delinquere aventi lo scopo di commettere taluno dei delitti ambientali previsti dal codice penale. Se si tratta di reato di associazione mafiosa, costituisce aggravante il fatto stesso dell'acquisizione della gestione o del controllo di attività economiche, di concessioni, autorizzazioni, appalti o di servizi pubblici in materia ambientale.

Reati concernenti specie animali o vegetali selvatiche protette o habitat protetti (artt. 727-bis e 733-bis c.p.)

Sono punite le condotte di prelievo, possesso, uccisione o distruzione di esemplari appartenenti a specie animali o vegetali selvatiche protette, fuori dei casi consentiti dalla legge e salvo che si tratti di danni considerati trascurabili, per quantità di esemplari o per impatto sullo stato di conservazione della specie. E' altresì punita la condotta di distruzione o di deterioramento tale da compromettere lo stato di conservazione di un habitat situato all'interno di un sito protetto. Le norme comunitarie elencano le specie animali o vegetali protette e individuano le caratteristiche che impongono la classificazione da parte della legge nazionale di un habitat naturale o di specie come zona a tutela speciale o zona speciale di conservazione.

Violazioni della disciplina degli scarichi (art. 137, commi 2, 3, 5, 11 e 13, C. A.)

L'art. 137 C. A. punisce una serie di violazioni della disciplina degli scarichi ed in particolare: gli scarichi senza autorizzazione di acque reflue industriali contenenti determinate sostanze pericolose, oppure in difformità delle prescrizioni dell'autorizzazione o nonostante la sua sospensione o revoca, nonché gli scarichi di sostanze pericolose oltre i valori limite; le violazioni dei divieti di scarico sul suolo, nelle acque sotterranee e nel sottosuolo fuori dalle ipotesi ammesse dagli artt. 103 e 104 C.A..

Infine, sono sanzionate le violazioni dei divieti di scarichi in mare effettuati da navi o aerei di sostanze pericolose previste dalle convenzioni internazionali, salvo che si tratti di scarichi autorizzati di quantità rapidamente biodegradabili..

Violazioni della disciplina sulla gestione dei rifiuti (art. 256, commi 1, 3, 5 e comma 6, 1° periodo, C.A.)

Le condotte punite consistono nella raccolta, trasporto, recupero, smaltimento commercio o intermediazione di rifiuti senza le prescritte autorizzazioni, iscrizioni all'Albo nazionale gestori ambientali e comunicazioni alle competenti autorità, oppure in difformità delle disposizioni contenute nelle autorizzazioni o impartite dalle autorità o in carenza dei requisiti prescritti.

Sono altresì punite le attività di realizzazione o gestione di una discarica non autorizzata, di miscelazione di rifiuti pericolosi di diverso genere tra di loro o con rifiuti non pericolosi e di deposito

di rifiuti sanitari pericolosi presso il luogo di produzione, per quantitativi superiori a 200 litri o equivalenti.

Omissione di bonifica per i casi di inquinamento del suolo, del sottosuolo, delle acque superficiali o sotterranee (art. 257, commi 1 e 2, C. A.)

Salvo che il fatto non costituisca più grave reato (ad es. quello di cui sopra all'art. 452-*bis* c.p.) è punito chi avendo cagionato l'inquinamento in oggetto con il superamento delle concentrazioni soglia di rischio non provvede alle dovute comunicazioni alle competenti autorità e alla bonifica del sito ai sensi dell'art. 242 C. A.. L'effettuazione della bonifica costituisce condizione di non punibilità anche per le contravvenzioni ambientali previste da altre leggi speciali per il medesimo evento.

Falso in certificato di analisi rifiuti (art. 258, comma 4, 2° periodo, C. A.)

Commette il delitto in questione chi fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti riportate in un certificato di analisi dei rifiuti e chi utilizza il certificato falso per il trasporto dei rifiuti.

Traffico illecito di rifiuti (art. 259, comma 1, C. A.)

La norma punisce chi effettua una spedizione di rifiuti transfrontaliera in violazione del Regolamento CE n. 259/93, che peraltro è stato abrogato e sostituito dal Regolamento CE n. 1013/2006.

Attività organizzate per il traffico illecito di rifiuti (art. 260, commi 1 e 2, C. A.)

Tale delitto è commesso da chi, al fine di conseguire un ingiusto profitto, cede, riceve, trasporta, esporta, importa o comunque gestisce abusivamente ingenti quantitativi di rifiuti. Deve trattarsi di fatti non episodici, ma di attività continuative, per lo svolgimento delle quali siano stati predisposti appositi mezzi ed organizzazione. E' prevista un'aggravante di pena per il caso di rifiuti altamente radioattivi.

Falsità nella tracciabilità dei rifiuti mediante il SISTRI (art. 260-bis, comma 6 – comma 7, 2° e 3° periodo - comma 8, C. A.)

Al sistema informatico di controllo della tracciabilità dei rifiuti, denominato SISTRI, partecipano obbligatoriamente o su base volontaria, secondo i criteri di cui all'art. 188-ter C.A., i produttori di rifiuti e gli altri soggetti che intervengono nella loro gestione (commercianti, intermediari, consorzi di recupero o riciclaggio, soggetti che compiono operazioni di recupero o di smaltimento, trasportatori). In tale contesto sono puniti i delitti consistenti nel fornire false indicazioni sulla natura e sulle caratteristiche di rifiuti al fine della predisposizione di un certificato di analisi dei rifiuti da

inserire in SISTRI, nell'inserire nel sistema un certificato falso o nell'utilizzare tale certificato per il trasporto dei rifiuti.

E' altresì punito il trasportatore che accompagna il trasporto con una copia cartacea fraudolentemente alterata della scheda SISTRI compilata per la movimentazione dei rifiuti.

Violazioni della disciplina delle emissioni in atmosfera (art. 279, comma 5, C. A.)

La norma punisce le emissioni in atmosfera compiute nell'esercizio di uno stabilimento, superiori ai valori limite stabiliti dalla legge o fissati nelle autorizzazioni o prescrizioni delle competenti autorità, quando siano superati anche i valori limite di qualità dell'aria previsti dalla vigente normativa.

Violazioni in tema di commercio e detenzione di animali o vegetali in via di estinzione o di mammiferi e rettili pericolosi (L. n. 150/1992, art. 1, commi 1 e 2 – art. 2, commi 1 e 2 – art. 3-bis, comma 1 - art. 6, comma 4)

Gli illeciti consistono nell'importazione, esportazione, trasporto, detenzione di esemplari di animali o di vegetali in violazione delle disposizioni comunitarie e internazionali che impongono particolari autorizzazioni, licenze e certificazioni doganali, e nella falsificazione o alterazione dei predetti documenti. E' vietata altresì la detenzione di determinati mammiferi e rettili pericolosi.

Sostanze lesive dell'ozono stratosferico (L. n. 549/1993, art. 3, comma 6)

La legge vieta il commercio, l'utilizzo, l'importazione, l'esportazione, la detenzione di sostanze lesive dell'ozono atmosferico dalla stessa elencate.

Inquinamento provocato dalle navi (D.Lgs. n. 202/2007, artt. 8 e 9)

La norma sanziona i comandanti delle navi, i membri dell'equipaggio, i proprietari e gli armatori che dolosamente o colposamente sversano in mare idrocarburi o sostanze liquide nocive trasportate alla rinfusa, fatte salve le deroghe previste.

7.10.2 Attività aziendali sensibili

Con riferimento all'operatività della SGR, i rischi di commissione dei reati ambientali possono presentarsi più verosimilmente con riferimento alla produzione di rifiuti, agli scarichi, alle emissioni in atmosfera e all'inquinamento del suolo.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia ambientale. Tale protocollo si completa con la normativa aziendale di dettaglio che regola l'attività medesima.

Si rimanda altresì ai protocolli previsti al Capitolo 7.2:

- “Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione”;
- “Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali”, che contengono principi di controllo e principi di comportamento diretti a prevenire anche la commissione dei reati di cui al presente Capitolo.

Detti protocolli si applicano anche a presidio delle attività esternalizzate o parzialmente esternalizzate sulla base di appositi contratti di servizio.

7.10.2.1 Gestione dei rischi in materia ambientale

Premessa

Il presente protocollo si applica a tutte le Strutture coinvolte nella gestione dei rischi in materia ambientale.

Coerentemente col proprio Codice Etico che individua la tutela dell'ambiente tra i propri valori di riferimento, il Gruppo Intesa Sanpaolo ha adottato una specifica Politica Ambientale.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi a quelli adottati dalla Capogruppo e recepiti da FIDEURAM – Intesa Sanpaolo Private Banking, risultano applicati anche a presidio di tutte le attività esternalizzate, sulla scorta dei relativi contratti di outsourcing.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Ai fini del presidio dei rischi in materia ambientale si rimanda ai seguenti processi:

Gestione dei locali della Società:

- gestione e manutenzione dei locali;
- pianificazione lavori;
- esecuzione lavori.

Gestione degli adempimenti legislativi in tema di rifiuti:

- gestione dei rifiuti.

Gestione della spesa e degli acquisti:

- ciclo passivo;
- gestione dell'approvvigionamento (delivery);
- sourcing.

Le modalità operative per la gestione dei processi sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti nell'ambito del processo:
 - per quanto attiene l'acquisto di beni e servizi, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
 - ogni trasporto di rifiuti speciali deve essere accompagnato da un formulario d'identificazione sottoscritto dal trasportatore e, per quanto attiene la SGR, da soggetti appositamente incaricati;
 - l'eventuale affidamento a terzi - da parte dei fornitori della SGR - di attività in sub-appalto, è contrattualmente subordinato a un preventivo assenso da parte della Struttura della SGR che ha stipulato il contratto ed al rispetto degli specifici obblighi sul rispetto della normativa ambientale.
- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi in materia ambientale. In particolare:
 - con riferimento ai locali della SGR, le Strutture operative che hanno il compito di realizzare e di gestire gli interventi quali servizi alla persona, servizi agli edifici, manutenzioni edili, opere edilizie/impiantistiche ed altri servizi integrati (es.: fornitura toner, gestione infermerie, ecc.) sono distinte e separate dalle Strutture alle quali sono attribuiti compiti di consulenza in tema di valutazione dei rischi ambientali e di controllo sulle misure atte a prevenirli e a ridurli.
- Attività di controllo:
 - il formulario d'identificazione dei rifiuti speciali compilato e sottoscritto dal trasportatore deve essere verificato dal soggetto incaricato dalla SGR;
 - verifica a campione sulla corretta gestione dei rifiuti con particolare riguardo a quelli speciali e, se presenti, a quelli pericolosi da parte delle Strutture competenti;

- verifica sulla corretta gestione da parte dell'appaltatore dei rifiuti derivanti dalle attività di manutenzione ordinaria e straordinaria e da ristrutturazioni dei locali della SGR. In particolare l'appaltatore è tenuto a ritirare a propria cura gli “scarti” dal proprio ciclo di lavoro e i Responsabili o soggetti all'uopo incaricati delle Unità Operative dove si svolgono il lavori devono vigilare sul corretto operato degli appaltatori evitando l'abbandono presso i locali della SGR dei rifiuti prodotti;
 - controllo sul corretto espletamento, da parte dei fornitori, dei servizi di manutenzione/pulizia (servizi agli edifici, servizi alle persone, ecc.) dei locali della SGR, con particolare riguardo alla regolare tenuta dei libretti degli impianti delle caldaie e dei gruppi frigoriferi nonché ai report manutentivi periodici redatti dai fornitori che hanno in appalto i servizi suddetti (es.: rapporti della “prova di tenuta” dei serbatoi per lo stoccaggio del gasolio).
- Tracciabilità del processo sia a livello di sistema informativo, sia in termini documentali:
 - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
 - documentabilità di ogni attività inerente ai processi con particolare riferimento alla corretta tenuta e conservazione dei libretti degli impianti delle caldaie e dei gruppi frigoriferi secondo quanto previsto dalla normativa vigente, specie relativamente alle loro emissioni;
 - conservazione nei termini di legge (cinque anni dall'ultima registrazione) del formulario d'identificazione dei rifiuti speciali e del registro di carico e scarico dei rifiuti pericolosi;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente all'esecuzione degli adempimenti svolti nell'ambito dei processi sopra descritti.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione dei rischi in materia ambientale oggetto del protocollo come pure tutti i dipendenti, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare, tutte le Strutture sono tenute – nei rispettivi ambiti - a:

- vigilare, per quanto di competenza, sul rispetto degli adempimenti in materia ambientale, in particolare sull'osservanza delle norme operative sul raggruppamento e deposito temporaneo dei rifiuti secondo la loro classificazione, sulla consegna ai trasportatori incaricati e sulla gestione di caldaie e gruppi frigoriferi;
- astenersi dall'affidare incarichi/appalti a eventuali consulenti esterni e/o fornitori eludendo criteri documentabili e obiettivi incentrati su professionalità qualificata, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia ambientale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto;
- prevedere, nell'ambito dei contratti di appalto, d'opera e di fornitura di servizi alla persona, agli edifici, manutenzioni edili, opere edilizie/impiantistiche ed altri servizi integrati (es.: fornitura toner, gestione infermerie, ecc.) specifiche clausole sul rispetto della normativa ambientale;
- nell'ambito delle procedure acquisitive di prodotti, macchine e attrezzature, che a fine ciclo vita potrebbero essere classificati potenzialmente pericolosi per l'ambiente, le Strutture committenti e la Struttura competente dedicata agli acquisti deve ottenere preventivamente dal potenziale fornitore la "scheda di pericolosità del prodotto" ed il codice CER da utilizzare per il corretto smaltimento dello stesso;
- considerare come requisito rilevante per la valutazione del fornitore, ove la natura della fornitura lo renda possibile e opportuno, le certificazioni ambientali;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es, A.S.L., Vigili del Fuoco, ARPA, Comune, Provincia, ecc.) in occasione di accertamenti/procedimenti ispettivi.

Parimenti, tutti i dipendenti sono tenuti a:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle Strutture aziendali e dalle Autorità competenti;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, qualsiasi situazione di emergenza ambientale (es.: sversamenti di gasolio, gravi malfunzionamenti degli impianti che provocano rumore esterno oltre i valori limite).

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- depositare i rifiuti al di fuori dal “Deposito Temporaneo Rifiuti” e consegnare i rifiuti speciali così come definiti dalla vigente normativa interna a fornitori incaricati del trasporto che non siano censiti nell’elenco delle Società autorizzate alla gestione dei rifiuti.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l’efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.