MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

DI

TEAMSYSTEM S.P.A.

AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

"Responsabilità amministrativa della Società"

DOCUMENTO APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE DEL 22 GIUGNO 2017

INDICE

DEFINIZIONI

DECRETO:	il Decreto Legislativo 8 giugno 2001, n. 231[1]
DIPENDENTI:	persone sottoposte alla direzione od alla vigilanza di uno dei soggetti apicali; quindi, ma non solo, tutti i soggetti – compresi i dirigenti - che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società nonché i lavoratori in distacco o in forza con contratti di lavoro parasubordinato;
DOCUMENTO INFORMATICO:	qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati a rielaborarli;
ILLECITI AMMINISTRATIVI:	gli illeciti amministrativi di cui all'art. 187-*quinquies* del Testo unico delle disposizioni in materia di intermediazione finanziaria (T.U.F.);
LINEE GUIDA DI CONFINDUSTRIA:	le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001 approvate da Confindustria in data 7 marzo 2002 (aggiornate a marzo 2014);
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO O MODELLO ORGANIZZATIVO:	il presente Modello di organizzazione, gestione e controllo così come previsto *ex* D.Lgs. 231/2001;
ORGANISMO DI VIGILANZA O ODV:	l'Organismo di vigilanza previsto dal D.Lgs. 231/2001;
REATI:	i reati di cui al Decreto legislativo 8 giugno 2001, n. 231;
SOCIETÀ:	TeamSystem S.p.A.
SOGGETTI APICALI:	persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione od il controllo della Società.

[1] E successive integrazioni e modificazioni: tale precisazione vale per qualsivoglia legge, regolamento o complesso normativo, che siano richiamati nel Modello.

Premessa

Il presente documento contiene la descrizione dei contenuti del Modello di Organizzazione, Gestione e Controllo ("**Modello Organizzativo**" o semplicemente "**Modello**") adottato da TeamSystem S.p.A. ("**TeamSystem**" o la "**Società**") con delibera del Consiglio di Amministrazione del 16 marzo 2017, ai sensi del D.lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni ("**D.lgs. 231/2001**" o "**Decreto**"), recante la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica. Il Modello Organizzativo è stato, quindi, successivamente aggiornato con delibera del CdA del 22 giugno 2017, allo scopo di adeguarne i contenuti alle modifiche normative apportate dal decreto legislativo 15 marzo 2017, n. 38, recante "*Attuazione della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato*" (G.U. n. 75 del 30 marzo 2017), in vigore a far data dal 14 aprile 2017.

Il presente documento contiene le linee guida ed i principi generali di adozione descrittivi del Modello e si compone di una "**Parte Generale**", nonché di singole "**Parti Speciali**" e dei relativi allegati.

La Parte Generale contiene una sintetica illustrazione del Decreto e dei suoi contenuti, oltre alle regole ed i principi generali del Modello; l'identificazione dell'Organismo di Vigilanza e la definizione dei compiti, poteri e funzioni di tale organismo; la descrizione del sistema sanzionatorio e disciplinare; la definizione di un sistema di comunicazione, informazione e formazione sul Modello; nonché la previsione di verifiche periodiche e dell'aggiornamento del Modello.

Le singole Parti Speciali contengono l'individuazione delle fattispecie di reato ritenute rilevanti per la Società, delle relative attività e processi a rischio, nonché la descrizione dei protocolli preventivi adottati in merito a ciascuna categoria di reato ritenuta rilevante per la Società.

SEZIONE PRIMA

1 Il Decreto Legislativo 231/2001

1.1 La Responsabilità Amministrativa degli Enti

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto Legislativo n. 231 (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia ha già da tempo aderito, ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Con tale Decreto, dal titolo "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", è stato introdotto nell'ordinamento italiano un regime di responsabilità amministrativa a carico di enti (società, associazioni, ecc. di seguito denominati "Enti") per alcuni reati commessi, nell'interesse o vantaggio degli stessi 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;
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità amministrativa degli Enti si aggiunge a quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'Ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o non risulti punibile.

1.2 I reati previsti dal Decreto

I reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell'ente, sono quelli espressamente e tassativamente richiamati dal Decreto e successive modifiche ed integrazioni.

Nell' "Allegato A – Fattispecie dei Reati", sono elencati tutti i reati attualmente ricompresi nell'ambito di applicazione del Decreto.

1.3 Le sanzioni previste dal Decreto

Il sistema sanzionatorio, a fronte del compimento dei reati sopra elencati, prevede l'applicazione delle seguenti sanzioni amministrative:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;

- pubblicazione della sentenza.

La sanzione pecuniaria è ridotta nel caso in cui: a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità, o se, prima della dichiarazione di apertura del dibattimento in primo grado: c) l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso e d) un Modello è stato adottato e reso operativo.

Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni: a) l'Ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti che ricoprono una posizione di rappresentanza, amministrativa o gestoria nell'Ente ovvero da soggetti sottoposti alla direzione al controllo dei primi e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; o b) in caso di reiterazione degli illeciti.

Il Decreto prevede le seguenti sanzioni interdittive, che possono avere una durata non inferiore a tre mesi e non superiore a due anni:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Ai sensi della vigente normativa, le sanzioni interdittive non si applicano in caso di commissione dei reati societari (con l'unica eccezione dei reati di corruzione tra privati ai sensi dell'art. 2635 co. 3 c.c. e di istigazione alla corruzione tra privati ai sensi dell'art. 2635-bis co. 1 c.c.) e di market abuse. Si precisa infatti che, per tali reati, sono previste le sole sanzioni pecuniarie, raddoppiate nel loro ammontare dall'art. 39, comma 5, della L. 262/2005 ("Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari").

Il Decreto prevede, inoltre, che, qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione interdittiva, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

1.4 Condizione esimente della Responsabilità amministrativa

Il Decreto prevede espressamente, agli artt. 6 e 7, l'esenzione dalla responsabilità amministrativa dell'Ente per reati commessi a proprio vantaggio e/o interesse qualora l'ente si sia dotato di effettivi ed efficaci modelli di organizzazione, gestione e controllo (di seguito anche il "**Modello**"), idonei a prevenire i medesimi fatti illeciti richiamati dalla normativa.

In particolare, nel caso in cui il reato venga commesso da Soggetti Apicali, l'Ente non risponde se prova che:

- l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curare il loro aggiornamento è stato affidato a un Organismo di Vigilanza dell'Ente dotato di autonomi poteri di iniziativa e controllo;
- le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione e gestione;
- vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza incaricato di vigilare sul funzionamento e sull'osservanza dei modelli di organizzazione e di gestione.

Per i reati commessi dai Sottoposti, l'Ente può essere chiamato a rispondere solo qualora venga accertato che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. In questa ipotesi, il Decreto riconduce la responsabilità ad un inadempimento dei doveri di direzione e vigilanza, che gravano tipicamente sul vertice aziendale (o sui soggetti da questi delegati).
L'inosservanza degli obblighi di direzione o vigilanza non ricorre se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

La semplice adozione del Modello da parte dell'organo dirigente non è, tuttavia, misura sufficiente a determinare l'esonero da responsabilità dell'ente medesimo, essendo piuttosto necessario che il Modello sia anche idoneo, efficace ed effettivo. A tal proposito il Decreto indica le caratteristiche essenziali per la costruzione di un modello di organizzazione gestione e controllo.

In particolare per la prevenzione dei reati il Modello deve (art. 6 comma 2 del Decreto):
- individuare e definire le attività aziendali nel cui ambito esiste la possibilità che vengano commessi reati previsti dal Decreto;
- predisporre specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- stabilire le modalità di reperimento e di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato a vigilare sul funzionamento e sull'osservanza del modello di organizzazione, gestione e controllo, al fine di consentirne la concreta capacità operativa;
- predisporre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo, al fine di garantirne l'effettività.

Inoltre, con riferimento all'efficace attuazione del Modello si prevede (art. 7 comma 4):
- una verifica periodica e l'eventuale modifica del Modello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
- l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

A tali requisiti devono aggiungersi, con riferimento ai reati commessi con violazione della normativa in materia di salute e sicurezza sul lavoro, quelli specificatamente dettati dall'art. 30, comma 1, del D.lgs. 9 aprile 2008, n. 81 ("**D.lgs. 81/08**"), secondo cui il Modello organizzativo deve essere tale da assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

a. al rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b. alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c. alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d. alle attività di sorveglianza sanitaria;
e. alle attività di informazione e formazione dei lavoratori;
f. alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
g. alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
h. alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il Modello deve, inoltre, prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra descritte, nonché un'articolazione di funzioni tale da assicurare le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve, altresì, prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo 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.

1.5 Le "Linee Guida" di Confindustria

L'art. 6 del Decreto dispone espressamente che il Modello possa essere adottato sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Le Linee Guida di Confindustria sono state approvate dal Ministero della Giustizia con il D.M. 4 dicembre 2003. Il successivo aggiornamento, pubblicato da Confindustria in data 24 maggio 2004, è stato approvato dal Ministero della Giustizia, che ha giudicato tali Linee Guida idonee al raggiungimento delle finalità previste dal Decreto. Dette Linee Guida sono state aggiornate da Confindustria alla data di marzo 2014.

Nella definizione del Modello, le Linee Guida di Confindustria prevedono le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare i reati previsti dal Decreto;
- la predisposizione di un sistema di controllo[2] (i c.d. protocolli) idoneo a prevenire i rischi di reato identificati nella fase precedente, attraverso la valutazione del sistema di controllo esistente all'interno dell'ente ed il suo grado di adeguamento alle esigenze espresse dal Decreto.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida di Confindustria per garantire l'efficacia del modello di organizzazione, gestione e controllo, sono le seguenti:

- la previsione di principi etici e di regole comportamentali in un codice etico;

[2] Il sistema di controllo esistente all'interno dell'ente, o sistema di controllo interno, "è *l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati*" (v. Codice di Autodisciplina, Comitato per la *Corporate Governance*, Borsa Italiana S.p.A., 2006, pag. 35).

- un sistema organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e descrizione dei compiti con specifica previsione di principi di controllo;
- procedure, manuali e/o informatiche, che regolino lo svolgimento delle attività, prevedendo opportuni controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, laddove richiesto, l'indicazione di limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

Il sistema di controllo, inoltre, deve conformarsi ai seguenti principi:

- verificabilità, tracciabilità, coerenza e congruità di ogni operazione;
- segregazione dei compiti (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli effettuati.

1.6 Delitti tentati e delitti commessi all'estero

L'Ente risponde anche degli illeciti dipendenti da delitti tentati e da reati commessi all'estero.

Nelle ipotesi di commissione nella forma del tentativo dei delitti previsti dal Decreto, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto.

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere, in relazione a reati – contemplati dallo stesso Decreto – commessi all'estero, al fine di non lasciare sfornita di sanzione una condotta criminosa di frequente verificazione, nonché al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

I presupposti su cui si fonda la responsabilità dell'Ente per reati commessi all'estero sono:

- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;
- l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
- le condizioni previste dagli artt. 7, 8, 9, 10 codice penale, con riferimento alla punibilità dei reati commessi all'estero, si devono essere verificate;
- non si procede nei confronti dell'Ente nello Stato in cui è stato commesso il fatto.

SEZIONE SECONDA

2 Il Modello di Organizzazione, Gestione e Controllo di TeamSystem S.p.A.

2.1 La Società

Con una presenza capillare e diffusa su tutto il territorio nazionale, TeamSystem S.p.A. (di seguito anche TeamSystem o la "Società") offre software e servizi ai clienti, sia direttamente attraverso le proprie sedi sia indirettamente attraverso una rete di Software Partner selezionati.

La rete commerciale e tecnica è costituita da professionisti altamente specializzati e con specifiche competenze di settore, in grado non solo di fornire un'assistenza al cliente di elevata qualità, ma anche di garantire la massima efficacia e personalizzazione delle soluzioni sulla base delle specifiche esigenze dell'utente finale.

La Società è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri soci e del lavoro dei propri dipendenti ed è consapevole dell'importanza di dotarsi di un sistema di controllo interno aggiornato ed idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, rappresentanti e partner d'affari.

A tal fine, TeamSystem ha avviato un Progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto e ad implementare il Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/01 (di seguito il "Modello").

Attraverso l'adozione del Modello, TeamSystem intende perseguire i seguenti obiettivi:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- diffondere la consapevolezza che dalla violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie (di natura pecuniaria e interdittiva) anche a carico della Società;
- consentire alla Società, grazie ad un sistema strutturato di procedure e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

2.2 Modello di Governance

La corporate governance di TeamSystem, basata sul modello tradizionale, è così articolata:

Assemblea degli azionisti, competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o dallo statuto.

Consiglio di Amministrazione, investito dei più ampi poteri per l'amministrazione della Società, con facoltà di compiere tutti gli atti opportuni per il raggiungimento degli scopi sociali, ad esclusione degli atti riservati – dalla legge e dallo statuto – all'Assemblea.

Collegio Sindacale, cui spetta il compito di vigilare: a) sull'osservanza della legge e dallo statuto nonché sul rispetto dei principi di corretta amministrazione; b) sull'adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del sistema amministrativo contabile, anche in riferimento all'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione; c) sull'adeguatezza delle disposizioni impartite alle Società controllate in relazione alle informazioni da fornire per adempiere agli obblighi di comunicazione.

Società di revisione, iscritta nell'albo speciale della Consob, che svolge l'attività di revisione contabile, incaricata dall'Assemblea degli azionisti.

2.3 Finalità del Modello

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventivo ed ex post) che abbia come obiettivo la riduzione del rischio di commissione dei reati mediante l'individuazione delle "Aree di attività a rischio" e dei "Processi strumentali/funzionali" alla commissione dei reati e la loro conseguente proceduralizzazione.

I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza nel potenziale autore del reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi di TeamSystem anche quando apparentemente essa potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a TeamSystem di reagire tempestivamente nel prevenire od impedire la commissione del reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare la consapevolezza nei Dipendenti, Organi Sociali, Società di Service, Consulenti e Partner, che operino per conto o nell'interesse della Società nell'ambito delle "Aree di attività a rischio" e dei "Processi strumentali/funzionali", di poter incorrere - in caso di comportamenti non conformi alle prescrizioni del Codice Etico e alle altre norme e procedure aziendali – in illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società.

Inoltre, si intende censurare fattivamente ogni comportamento illecito attraverso la costante attività dell'Organismo di Vigilanza sull'operato delle persone rispetto alle "Aree di attività a rischio" e ai "Processi strumentali/funzionali" e la comminazione di sanzioni disciplinari o contrattuali.

Gli elementi che caratterizzano il presente Modello sono: l'efficacia, la specificità e l'attualità.

L'efficacia

L'efficacia di un Modello dipende dalla sua idoneità in concreto ad elaborare meccanismi di decisione e di controllo tali da eliminare – o quantomeno ridurre significativamente – l'area di rischio da responsabilità. Tale idoneità è garantita dall'esistenza di meccanismi di controllo preventivo e successivo idonei ad identificare le operazioni che possiedono caratteristiche anomale, tali da segnalare condotte rientranti nelle aree di rischio e strumenti di tempestivo intervento nel caso di individuazione di siffatte anomalie. L'efficacia di un Modello, infatti, è anche funzione dell'efficienza degli strumenti idonei ad identificare "sintomatologie da illecito".

La specificità

La specificità di un Modello è uno degli elementi che ne connota l'efficacia.

- È necessaria una specificità connessa alle aree a rischio, così come richiamata dall'art. 6, comma 2 lett.a) del Decreto, che impone un censimento delle attività della Società nel cui ambito possono essere commessi i reati;
- Ai sensi dell'art. 6, comma 2 lett.b) del Decreto, è altrettanto necessario che il Modello preveda dei processi specifici di formazione delle decisioni dell'ente e dei processi di attuazione nell'ambito dei settori "sensibili".

Analogamente, l'individuazione delle modalità di gestione delle risorse finanziarie, l'elaborazione di un sistema di doveri d'informativa, l'introduzione di un adeguato sistema disciplinare sono obblighi che richiedono la specificità delle singole componenti del Modello.

Il Modello, ancora, deve tener conto delle caratteristiche proprie, delle dimensioni della Società e del tipo di attività svolte, nonché della storia della Società.

L'attualità

Un Modello è idoneo a ridurre i rischi da reato qualora sia costantemente adattato ai caratteri della struttura e dell'attività d'impresa.

In tal senso l'art. 6 del Decreto prevede che l'Organismo di Vigilanza, titolare di autonomi poteri d'iniziativa e controllo, abbia la funzione di supervisionare all'aggiornamento del Modello.

L'art. 7 del Decreto stabilisce che l'efficace attuazione del Modello contempli una verifica periodica, nonché l'eventuale modifica dello stesso allorquando siano scoperte eventuali violazioni oppure intervengano modifiche nell'attività o nella struttura organizzativa della Società.

2.4 Destinatari

Le regole contenute nel Modello si applicano:

- a coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale, amministratore, membro del collegio sindacale;
- a coloro i quali svolgano funzioni di direzione in veste di responsabili di specifiche Unità Organizzative;
- a coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società.
- ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale, ancorché distaccati all'estero per lo svolgimento dell'attività;
- a chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima.

Il Modello costituisce un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di materiali, servizi e lavori, consulenti, partners con cui TeamSystem opera.

2.5 Struttura del Modello

Il Modello è formato da tutte le "componenti" individuate nel paragrafo 2.6 che segue e da tutte le procedure, le policies aziendali e di gruppo ed i sistemi di gestione e controllo richiamati e/o previsti nel presente documento.

Il presente documento si compone di una "Parte Generale" e da singole "Parti Speciali" predisposte per le diverse tipologie di reato contemplate nel Decreto.

Si evidenzia che nelle Parti Speciali sono state riportate le tipologie di reato presupposto, identificate nell'ambito di un'attività di mappatura delle "Aree a rischio reato" e per le quali è stato ritenuto che TeamSystem sia, in via potenziale ed eventuale, esposta al rischio di commissione degli illeciti in considerazione delle attività svolte.

È demandato al Consiglio di Amministrazione di TeamSystem di integrare il presente Modello in una successiva fase, mediante apposite delibere, con ulteriori Parti Speciali relative ad altre tipologie di reato che, per effetto di altre normative, risultino inserite o comunque collegate all'ambito di applicazione del Decreto.

E' opportuno precisare che il presente documento individua e riassume il contenuto descrittivo ed i principi generali di adozione del Modello, essendo la individuazione dei sistemi di prevenzione dei rischi concretamente definita anche attraverso il rinvio agli strumenti di controllo utilizzati nella realtà operativa aziendale (tra cui procedure, istruzioni operative, policies, sistemi autorizzativi, struttura organizzativa, sistema delle deleghe e delle procure, norme di comportamento, modalità di gestione delle risorse finanziarie, strumenti di tracciabilità e documentazione, etc.), da intendersi integralmente richiamati nel presente Modello. Ed infatti, ragioni di "praticabilità" e funzionalità dello stesso Modello Organizzativo impongono di non trascrivere pedissequamente e materialmente all'interno del presente documento l'intero sistema delle procedure e degli ulteriori controlli in essere, tanto più ove si consideri che tali strumenti di controllo operativo costituiscono un

"corpo vivo", dinamico ed in costante evoluzione, soggetto ad esigenze di aggiornamento proprio allo scopo di garantirne l'efficacia e l'attualità. Ciononostante, tali procedure e sistemi di controllo devono intendersi qui richiamati quale parte integrante ed essenziale del Modello Organizzativo, del quale costituiscono il nucleo "operativo".

Anche le azioni di miglioramento del sistema di controllo interno attuate successivamente all'adozione del Modello Organizzativo costituiscono a tutti gli effetti parte integrante del Modello Organizzativo stesso, nonché del sistema dei protocolli preventivi adottati a presidio delle diverse aree ed attività a rischio.

2.6 Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali sviluppati da TeamSystem nella definizione del Modello, possono essere così riassunti:

- mappatura delle attività sensibili[3], con esempi di possibili modalità di realizzazione dei reati e dei processi strumentali/funzionali potenzialmente associabili alla commissione dei reati richiamati dal Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico;
- identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal Decreto, sancite nel Codice Etico adottato dalla Società e, più in dettaglio, nel presente Modello;
- nomina di un Organismo di Vigilanza al quale sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello ai sensi dell'art. 6 punto b) del Decreto;
- approvazione di un sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione, sensibilizzazione e divulgazione ai Destinatari del presente Modello;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso (cfr. par. 5 "Aggiornamento del Modello").

2.7 Codice Etico e Modello

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice stesso. Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte della Società allo scopo di esprimere dei principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti;
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi apparentemente a vantaggio dell'azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

---

[3] Tramite l'analisi documentale e le interviste svolte, con i soggetti aziendali informati dell'organizzazione e delle attività svolte dalle Funzioni/Direzioni, nonché dei processi aziendali nei quali le attività sono articolate, sono identificate:

- le aree di attività "sensibili" alla commissione dei reati, o aree di attività a potenziale rischio-reato ai sensi del Decreto;
- i processi "strumentali/funzionali" alla realizzazione dei reati di cui al Decreto, o processi nel cui ambito potrebbero crearsi le condizioni e/o gli strumenti per la commissione del reato.

2.8 Presupposti del Modello

Nella predisposizione del Modello, TeamSystem ha tenuto conto della propria organizzazione aziendale, al fine di verificare le aree di attività più esposte al rischio di potenziale commissione di reati.

La Società ha tenuto altresì conto del proprio sistema di controllo interno al fine di verificarne la capacità a prevenire le fattispecie di reato previste dal Decreto nelle aree di attività identificate a rischio.

Più in generale, il sistema di controllo interno di TeamSystem deve garantire, con ragionevole certezza, il raggiungimento di obiettivi operativi, di informazione e di conformità:

- l'obiettivo operativo del sistema di controllo interno riguarda l'efficacia e l'efficienza della Società nell'impiegare le risorse, nel proteggersi dalle perdite, nel salvaguardare il patrimonio aziendale; tale sistema è volto, inoltre, ad assicurare che il personale operi per il perseguimento degli obiettivi aziendali, senza anteporre altri interessi a quelli di TeamSystem;
- l'obiettivo di informazione si traduce nella predisposizione di rapporti tempestivi ed affidabili per il processo decisionale all'interno e all'esterno dell'organizzazione aziendale;
- l'obiettivo di conformità garantisce, invece, che tutte le operazioni ed azioni siano condotte nel rispetto delle leggi e dei regolamenti, dei requisiti prudenziali e delle procedure aziendali interne.

In particolare, il sistema di controllo interno si basa sui seguenti elementi:

- sistema organizzativo formalizzato e chiaro nell'attribuzione delle responsabilità;
- sistema procedurale;
- sistemi informatici orientati alla segregazione delle funzioni;
- sistema di controllo di gestione e reporting;
- poteri autorizzativi e di firma assegnati in coerenza con le responsabilità;
- sistema di comunicazione interna e formazione del personale.

Alla base del sistema di controllo interno di TeamSystem vi sono i seguenti principi:

- ogni operazione, transazione e azione deve essere veritiera, verificabile, coerente e documentata;
- nessuno deve poter gestire un intero processo in autonomia (c.d. segregazione dei compiti);
- il sistema di controllo interno deve poter documentare l'effettuazione dei controlli, anche di supervisione.

Tutto il personale, nell'ambito delle funzioni svolte, è responsabile della definizione e del corretto funzionamento del sistema di controllo attraverso i controlli di linea, costituiti dall'insieme delle attività di controllo che le singole unità operative svolgono sui loro processi. Modifiche del Modello

Tutte le modifiche e le integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del Consiglio di Amministrazione della Società, essendo il presente Modello un atto di emanazione dell'organo dirigente (cfr. Decreto, Art. 6).

Al fine di garantire la stabilità e l'effettività del Modello, le decisioni per le modifiche ed integrazioni sostanziali del Modello devono essere approvate con il voto favorevole di almeno due terzi degli amministratori presenti alla seduta.

2.9 Individuazione delle attività "a rischio"

La predisposizione del Modello è stata preceduta da una serie di attività propedeutiche in linea con le previsioni del Decreto.

Il Decreto prevede espressamente, al relativo art. 6, comma 2, lett. a), che il Modello dell'ente individui, infatti, le attività aziendali, nel cui ambito possano essere potenzialmente commessi i reati di cui al medesimo Decreto.

Nel rispetto di tali requisiti, i modelli di organizzazione e gestione possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative di categoria e giudicati idonei dal Ministero della Giustizia.

La Società ha condotto un'attenta analisi dei propri strumenti di organizzazione, gestione e controllo, diretta a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto e, ove si sia reso necessario, ad adeguarli.

A seguito di tale analisi, la Società ha condotto un processo di miglioramento del proprio sistema di controllo interno allo scopo di sanare le criticità evidenziate nel corso delle attività di risk assessment, ad esempio, procedendo alla formalizzazione delle procedure operative destinate a regolare i processi strumentali e dotandosi di policy e protocolli interni a presidio delle attività a rischio, che costituiscono parte integrante e sostanziale del presente Modello Organizzativo.

In considerazione delle attività caratteristiche di TeamSystem, le aree a rischio rilevate hanno riguardato, in particolar modo, i reati previsti dagli artt. 24 e 25, 24 bis, 25 bis/1, 24 ter, 25 ter, 25 sexies, 25 septies, 25 octies, 25 novies, 25 decies, 25 undecies, 25 duodecies.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti dal Decreto (cd. mappatura), come già sopra ricordato, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I risultati dell'attività di mappatura sopra descritta, previamente condivisi con i referenti aziendali intervistati, sono stati raccolti in una scheda descrittiva (c.d. Matrice delle attività a rischio – reato), che illustra nel dettaglio i concreti profili di rischio di commissione dei reati richiamati dal Decreto, nell'ambito delle attività della Società.

Nello specifico, è stato riscontrato il rischio di possibile commissione dei reati previsti dal Decreto nelle seguenti aree di attività aziendale:

- Gestione dei rapporti di "alto profilo" con soggetti appartenenti alla Pubblica Amministrazione
    - Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (es. Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni).

- Gestione degli adempimenti, delle comunicazioni e delle richieste, anche in occasione di verifiche, ispezioni ed accertamenti da parte degli enti pubblici competenti o delle autorità amministrative indipendenti
    - Gestione di rapporti con i Funzionari pubblici e adempimenti presso enti istituzionali competenti, quali ad es.
        - ✓ rapporti con i funzionari della Guardia di Finanza, dell'Agenzia delle Entrate e degli Enti competenti in materia fiscale, tributaria anche in occasione di verifiche, ispezioni e accertamenti;

- ✓ adempimenti presso l'Ufficio Brevetti del Ministero dello Sviluppo Economico per l'espletamento delle attività previste nell'ambito della domanda di brevetto per un software elaborato dalla Società.

- Rapporti con le Autorità Amministrative Indipendenti (es. Autorità Garante della Concorrenza e del mercato) e gestione delle comunicazioni e delle informazioni a esse dirette, anche in occasione di verifiche ispettive.

- Gestione dei rapporti con gli enti pubblici competenti per l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione
  - Gestione dei rapporti con Funzionari degli Enti Pubblici finanziatori, internazionali, nazionali e locali (es. Comunità Europea, Regione, Provincia), per il conseguimento, a titolo esemplificativo, di finanziamenti, anche a fondo perduto, contributi o erogazioni pubbliche finalizzati alla realizzazione di progetti di formazione in sede di:
    - ✓ ottenimento delle informazioni connesse ai bandi di gara
    - ✓ presentazione della richiesta;
    - ✓ verifiche e accertamenti circa il corretto utilizzo del finanziamento
  - Predisposizione e trasmissione della documentazione per la richiesta del finanziamento (es. documentazione amministrativa richiesta dal bando, documentazione tecnica, etc.) e/o della documentazione di rendicontazione.
  - Gestione del finanziamento in termini di utilizzo dello stesso.

- Gestione degli adempimenti in materia di assunzioni, cessazione del rapporto di lavoro, retribuzioni, ritenute fiscali e contributi previdenziali e assistenziali, relativi a dipendenti e collaboratori
  - Gestione dei rapporti con i Funzionari Pubblici in occasione di verifiche circa il rispetto dei presupposti e delle condizioni (ad es. piano formativo, durata, rispetto dei limiti d'età, ecc.) richieste dalla normativa vigente per le assunzioni agevolate.
  - Gestione dei rapporti, anche tramite consulenti esterni, con funzionari competenti (INPS, INAIL, ASL, Direzione Provinciale del Lavoro ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento, anche in occasione di verifiche ispettive:
    - ✓ predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro;
    - ✓ autorizzazione per l'assunzione di personale appartenente a categorie protette;
    - ✓ elenchi del personale attivo, assunto e cessato presso l'INAIL;
    - ✓ controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente.

- Selezione e assunzione del personale
  - Gestione delle attività di selezione, assunzione e gestione del personale con particolare riferimento a titolo esemplificativo alle seguenti attività:
    - ✓ definizione del piano di fabbisogno del personale;
    - ✓ richiesta di assunzione;
    - ✓ screening dei cv;

- ✓ analisi delle candidature;
- ✓ formalizzazione del contratto di assunzione.

- Gestione dei contenziosi (es.: civili, tributari, giuslavoristici, amministrativi, penali), in tutti i gradi di giudizio
  - Gestione dei rapporti con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi (civile, penale, amministrativo, giuslavoristico e tributario) con particolare riferimento alla nomina dei legali esterni.
  - Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

- Gestione della contabilità generale e formazione del bilancio
  - Gestione della contabilità generale, con particolare riferimento alle attività di:
    - ✓ rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (es. gestione e registrazione contabile della fatturazione attiva);
    - ✓ verifica dati provenienti dai sistemi informativi alimentanti;
    - ✓ raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato

- Gestione dei flussi monetari e finanziari
  - Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività:
    - ✓ autorizzazione e invio dei pagamenti;
    - ✓ inserimento/modifica delle coordinate bancarie del fornitore.

- Gestione degli adempimenti in materia societaria
  - Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul Bilancio d'Esercizio e nelle attività di verifica della gestione aziendale.
  - Custodia e tenuta dei Libri Sociali.
  - Tenuta delle scritture contabili e dei libri contabili.
  - Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. Registro delle imprese presso le Camere di Commercio competenti).

- Gestione della sicurezza informatica
  - Gestione della sicurezza fisica e logica dei sistemi informativi aziendali. In particolare:
    - ✓ gestione dei server aziendali e delle applicazioni in uso presso la Società;
    - ✓ gestione della rete telematica

- ✓ manutenzione di client assegnati al personale dipendente della Società
- ✓ gestione delle credenziali di autenticazione;
- ✓ gestione dei profili di autorizzazione.

- Approvvigionamento di beni e servizi
  - Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività:
    - ✓ gestione dell'albo fornitori;
    - ✓ selezione del fornitore e valutazione dei requisiti qualificanti;
    - ✓ stipula di accordi quadro di fornitura;
    - ✓ emissione degli ordini.

- Progettazione e commercializzazione di software applicativi per elaboratori
  - Gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi.
  - Gestione dei rapporti con clienti diretti e distributori, con particolare riferimento alle seguenti attività:
    - ✓ gestione dell'anagrafica clienti;
    - ✓ definizione della scontistica da applicare;
    - ✓ formalizzazione dell'offerta;
    - ✓ evasione dell'ordine;
    - ✓ monitoraggio del credito.

- Gestione delle partnership
  - Gestione dei rapporti con società pubbliche e private con le quali si intende stipulare accordi di partnership, con particolare riferimento alle seguenti attività:
    - ✓ individuazione delle opportunità di partnership commerciali/tecnologiche;
    - ✓ definizione degli accordi con i Partner.

- Gestione delle attività infragruppo
  - Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo

- Gestione del sistema sicurezza ai sensi del D.Lgs. 81/08 (Testo Unico Sicurezza)
  - Gestione dei rapporti con le autorità in materia di tutela della sicurezza e salute sul lavoro, anche in occasione di verifiche e ispezioni, in occasione di, a titolo esemplificativo:
    - ✓ adempimenti previsti dal D.lgs. 81/2008 – Testo Unico sulla Sicurezza nei luoghi di lavoro;
    - ✓ relative ispezioni in materia di sicurezza, salute, igiene sul lavoro;

- ✓ ottenimento del Certificato Prevenzione Incendi;
- ✓ autorizzazione sanitaria.

  - Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza sul lavoro ai sensi del D.Lgs. 81/2008 - Testo Unico sulla Sicurezza nei luoghi di lavoro e successive modifiche ed integrazioni.

- Gestione dei rifiuti
  - Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti.

- Relazioni con il mercato
  - Redazione e trasmissione di documenti informativi, prospetti informativi, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e le altre appartenenti al Gruppo, destinate agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale.

Sono stati anche individuati i processi nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato (processi c.d. strumentali) e i processi che sovraintendono direttamente le attività sensibili (processi c.d. funzionali):

- Consulenze e incarichi professionali a terzi;
- Acquisto di beni e servizi;
- Rimborsi spese, anticipi e spese di rappresentanza;
- Flussi monetari e finanziari;
- Gestione del contenzioso;
- Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità;
- Selezione, assunzione, gestione del personale dipendente;
- Rapporti con la Pubblica Amministrazione;
- Formazione del Bilancio e adempimenti societari;
- Gestione della Sicurezza sul Lavoro;
- Gestione dei sistemi informativi;
- Gestione degli adempimenti in materia ambientale;
- Progettazione e commercializzazione di prodotti;
- Gestione delle informazioni privilegiate.

2.10 Principi di controllo interno generali e specifici

Il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di: esplicita formalizzazione delle norme comportamentali; chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna direzione e alle diverse qualifiche e ruoli professionali; precisa

descrizione delle attività di controllo e loro tracciabilità; adeguata segregazione di ruoli operativi e ruoli di controllo.

In particolare devono essere perseguiti i seguenti principi generali di controllo interno:

Norme comportamentali

- Esistenza di un Codice Etico che descriva regole comportamentali di carattere generale a presidio delle attività svolte.

Definizioni di ruoli e responsabilità

- La regolamentazione interna deve declinare ruoli e responsabilità delle unità organizzative a tutti i livelli, descrivendo in maniera omogenea, le attività proprie di ciascuna struttura;
- tale regolamentazione deve essere resa disponibile e conosciuta all'interno dell'organizzazione.

Procedure e norme interne

- Le attività sensibili devono essere regolamentate, in modo coerente e congruo, attraverso gli strumenti normativi aziendali, così che in ogni momento si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato;
- deve essere individuato e formalizzato un Responsabile per ciascuna attività sensibile, tipicamente coincidente con il responsabile della struttura organizzativa competente per la gestione dell'attività stessa.

Segregazione dei compiti

- All'interno di ogni processo aziendale rilevante, devono essere separate le funzioni o i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla;
- non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno.

Poteri autorizzativi e di firma

- Deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando l'impresa e manifestando la sua volontà;
- i poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- le procure devono essere coerenti con il sistema interno delle deleghe;
- sono previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni;
- il sistema di deleghe deve identificare, tra l'altro:
    - i requisiti e le competenze professionali che il delegato deve possedere in ragione dello specifico ambito di operatività della delega;
    - l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguente assunzione degli obblighi conferiti;

  - le modalità operativa di gestione degli impegni di spesa;
- le deleghe sono attribuite secondo i principi di:
  - autonomia decisionale e finanziaria del delegato;
  - idoneità tecnico-professionale del delegato;
  - disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- Nell'ambito delle procedure o di altra regolamentazione interna devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità);
- la documentazione afferente alle attività sensibili deve essere adeguatamente formalizzata e riportare la data di compilazione, presa visione del documento e la firma riconoscibile del compilatore/supervisore; la stessa deve essere archiviata in luogo idoneo alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti;
- devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate;
- il responsabile dell'attività deve produrre e mantenere adeguati report di monitoraggio che contengano evidenza dei controlli effettuati e di eventuali anomalie;
- deve essere prevista, laddove possibile, l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile e ai soggetti che vi partecipano. Il sistema deve prevedere l'impossibilità di modifica (non tracciata) delle registrazioni;
- i documenti riguardanti l'attività della Società, ed in particolare i documenti o la documentazione informatica riguardanti attività sensibili sono archiviati e conservati, a cura della direzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;
- l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a loro delegato, al Collegio Sindacale od organo equivalente o ad altri organi di controllo interno, alla società di revisione eventualmente nominata e all'Organismo di Vigilanza.

Principi specifici di controllo interno

Di seguito vengono enunciati, per i processi funzionali e/o strumentali individuati precedentemente, a titolo non esaustivo, i principi di controllo minimali a cui si deve ispirare l'operatività degli stessi.

In ogni caso, anche nell'ipotesi di esternalizzazione di processi e attività, presso la Società devono essere previsti poteri delegati e specifiche procure per coloro che operano in nome e per conto della Società, anche se in via temporanea e per particolari operazioni.

Per i processi "strumentali" identificati, anche nell'ipotesi di esternalizzazione, devono essere applicati dalla Società i principi nel seguito riportati.

Consulenze e Incarichi Professionali a terzi

- Deve essere prevista l'esistenza di attori diversi operanti nelle differenti fasi del processo di gestione delle consulenze (ad es. in linea di principio non vi deve essere coincidenza di identità tra chi richiede la consulenza, chi la autorizza e chi esegue il pagamento della prestazione);

- deve essere effettuata un'adeguata attività selettiva fra i diversi operatori di settore;
- devono essere utilizzati idonei dispositivi contrattuali adeguatamente formalizzati;
- devono esistere adeguati livelli autorizzativi (in coerenza con il sistema di procure aziendali) per la stipulazione dei contratti;
- devono essere presenti i livelli di approvazione per la formulazione delle richieste di consulenza e per la certificazione/validazione del servizio reso;
- devono esistere i requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e di meccanismi di valutazione complessiva del servizio reso;
- nell'impiego di consulenti esterni, nell'ambito della gestione dei rapporti con la PA, devono essere previsti dei meccanismi di verifica preventiva dell'assenza di contemporanea collaborazione sulla medesima materia con le stesse amministrazioni pubbliche (per esempio mediante auto-certificazione del consulente esterno);
- nei contratti con partner, consulenti e professionisti deve essere contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparati in procedimenti giudiziari relativi ai reati contemplati dalla presente Parte Generale;
- nei contratti di fornitura, patti fra soci o partners commerciali, deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- devono esistere documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e archiviati.

Acquisto di Beni e Servizi

- Devono esistere norme aziendali relative all'approvvigionamento di particolari tipologie di beni e servizi (consulenze, prestazioni professionali) ovvero relative ad approvvigionamenti con particolari modalità attuative (es. con riferimento al fornitore unico, o in caso di urgenza);
- le norme aziendali devono essere ispirate, in ciascuna fase del processo di approvvigionamento, a criteri di trasparenza (precisa individuazione dei soggetti responsabili, valutazione delle richieste di approvvigionamento, verifica che le richieste arrivino da soggetti autorizzati, determinazione dei criteri che saranno utilizzati nelle varie fasi del processo e tracciabilità delle valutazioni sulle offerte tecniche ed economiche) e di tracciabilità delle operazioni effettuate;
- la scelta della modalità di approvvigionamento da adottare (es. pubblicazione del bando, fornitore unico, utilizzo di vendor list qualificate) deve essere formalizzata e autorizzata a un adeguato livello gerarchico;
- deve essere garantito il rispetto dei compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo e dalle procedure vigenti nel processo di acquisto di beni e servizi;
- deve essere garantito il rispetto dei principi di correttezza e trasparenza e garanzia dell'integrità e della reputazione delle parti nei rapporti intrattenuti con i fornitori;
- deve essere garantita la tracciabilità e trasparenza nella definizione dell'esigenza di acquisto e nell'individuazione del fornitore;
- deve essere acquisito l'impegno formale da parte dell'affidatario dei lavori ad uniformarsi alle prescrizioni del Codice Etico ed alle linee di condotta del Modello al fine di sanzionare eventuali comportamenti contrari ai principi etici aziendali;
- deve essere ottenuta una dichiarazione di assenza di rapporti preesistenti tra il fornitore e la Pubblica Amministrazione ostativi all'affidamento della fornitura.

- deve essere identificata una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard.
- devono essere determinati adeguati criteri di selezione, selezione, stipulazione ed esecuzione di accordi/joint venture con altre imprese per la realizzazione di investimenti.

Rimborsi spese, anticipi e spese di rappresentanza

- Non devono essere ammessi anticipi o rimborsi delle spese sostenute direttamente dai soggetti esterni, in particolare da rappresentanti della Pubblica Amministrazione che beneficiano di ospitalità;
- la gestione dei rimborsi spese deve avvenire in accordo con la normativa, anche fiscale, applicabile;
- i processi di autorizzazione e controllo delle trasferte devono essere sempre ispirati a criteri di economicità e di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e delle normative fiscali vigenti;
- nello svolgimento di attività di servizio devono essere sempre ricercate le soluzioni più convenienti, sia in termini di economicità che di efficienza operativa;
- il sostenimento di spese di rappresentanza deve soddisfare il concetto di "opportunità" della spesa, in linea pertanto con gli obiettivi aziendali;
- le spese per forme di accoglienza e di ospitalità devono attenersi ad un criterio di contenimento dei costi entro limiti di normalità.

Flussi Monetari e Finanziari

- Deve essere assicurata la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi;
- deve essere sempre prevista la rilevazione e l'analisi di pagamenti/incassi ritenuti anomali per controparte, importo, tipologia, oggetto, frequenza o entità sospette;
- devono essere immediatamente interrotte o, comunque, non deve essere data esecuzione ad operazioni di incasso e pagamento che vedano coinvolti soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;
- devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone;
- le operazioni che comportano utilizzo o impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie devono avere sempre una causale espressa e essere documentate e registrate in conformità con i principi di professionalità e correttezza gestionale e contabile. Il processo operativo e decisionale deve essere tracciabile e verificabile nelle singole operazioni;
- deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza dei destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione; in particolare dovrà essere precisamente verificato che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- deve essere verificata la congruità delle provvigioni pagate ai collaboratori esterni (ad esempio agenti) rispetto a quelle praticate nell'area geografica di riferimento;
- deve essere previsto il divieto di utilizzo del contante, ad eccezione dell'uso per importi non significativi della cassa interna, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o

altro utilizzo di disponibilità finanziarie nonché il divieto di accettazione ed esecuzione di ordini di pagamento provenienti da soggetti non identificabili;

- per la gestione dei flussi in entrata e in uscita, devono essere utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione europea o enti creditizi/finanziari situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- devono essere vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minime di spesa espressamente autorizzate dalla funzione amministrazione, ed in particolare per le operazioni di piccola cassa.

Gestione del contenzioso

- Nell'ambito dell'organizzazione interna devono essere definiti:
  - i limiti delle deleghe di spesa dei soggetti coinvolti nella gestione del contenzioso;
  - i criteri di individuazione di legali esterni per la gestione dei contenziosi;
- l'articolazione del processo deve garantire la segregazione funzionale tra:
  - coloro che hanno la responsabilità di gestire il contenzioso, anche mediante l'ausilio di legali esterni;
  - coloro che hanno la responsabilità di imputare a budget le spese legali da sostenere;
  - coloro che hanno la responsabilità di verificare il rispetto delle deleghe di spesa e di poteri conferiti ed il rispetto dei criteri definiti per la scelta dei legali e la natura e la pertinenza degli oneri legali sostenuti;
- deve essere prevista la predisposizione di uno scadenzario che permetta di controllare l'intera attività esecutiva, con particolare riferimento al rispetto dei termini processuali previsti;
- deve essere garantita la tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate.

Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità

- Deve esistere una autorizzazione formalizzata a conferire utilità;
- devono esistere documenti giustificativi delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità, validati dal superiore gerarchico e archiviati;
- gli eventuali fornitori delle utilità devono essere scelti all'interno di una lista gestita dalla direzione competente. L'inserimento / eliminazione dei fornitori dalla lista deve essere basato su criteri oggettivi. L'individuazione, all'interno della lista, del fornitore della singola utilità deve essere motivata e documentata;
- è prevista la rilevazione di operazioni (donazioni, sponsorizzazioni, omaggi e liberalità) ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette;
- nei contratti di sponsorizzazione deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- deve essere verificata la regolarità dei pagamenti per donazioni, sponsorizzazioni o liberalità con riferimento alla piena coincidenza dei destinatari dei pagamenti e le controparti effettivamente coinvolte;

- sono immediatamente interrotte o, comunque, non è data esecuzione ad operazioni relative a donazioni, sponsorizzazioni, omaggi e liberalità, che vedano coinvolti come beneficiari, soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;
- devono esistere report periodici sulle spese per la concessione di utilità, con motivazioni e nominativi dei beneficiari, inviati al livello gerarchico superiore e archiviati.

Selezione, assunzione, gestione del personale dipendente

- La lettera di impegno all'assunzione e il relativo contratto di assunzione devono essere firmate dal soggetto a ciò autorizzato secondo i poteri di firma;
- devono definite caratteristiche e requisiti per le figure professionali oggetto di assunzioni;
- la Società può avvalersi esclusivamente di personale assunto in conformità alle tipologie contrattuali previste dalla normativa e dai contratti collettivi nazionali di lavoro applicabili;
- deve essere conservata evidenza documentale delle singole fasi del processo di selezione e assunzione del personale.
- la scelta dei dipendenti, dei consulenti e dei collaboratori deve avvenire a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile;
- deve essere preventivamente richiesto al candidato di dichiarare eventuali rapporti di parentela entro il secondo grado con esponenti della Pubblica Amministrazione e, in caso positivo, deve essere valutata l'eventuale sussistenza di ipotesi di conflitto di interessi;
- siano formalmente stabiliti ed efficacemente svolti controlli periodici e documentati sul calcolo e sul pagamento delle remunerazioni variabili;
- eventuali sistemi premianti ai dipendenti e collaboratori devono rispondere ad obiettivi realistici e coerenti con le mansioni, l'attività svolta e le responsabilità affidate.

Rapporti con la Pubblica Amministrazione

- Le funzioni interessate devono essere in possesso di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti;
- i rapporti con i Rappresentanti della Pubblica Amministrazione devono gestiti esclusivamente dai soggetti aziendali muniti degli occorrenti poteri in conformità al sistema di deleghe e procure, ovvero da coloro che siano da questi formalmente delegati, e in ogni caso nel rispetto delle procedure aziendali che regolano detti rapporti;
- tutti i contratti che hanno come controparte la Pubblica Amministrazione, nonché tutti gli atti, le richieste e le comunicazioni formali inoltrate alla Pubblica Amministrazione devono essere autorizzati, coordinati, gestiti e firmati da coloro che sono dotati di idonei poteri in base alle norme interne;
- deve essere redatta una verbalizzazione degli incontri particolarmente rilevanti con il rappresentante della Pubblica Amministrazione attraverso la redazione di un verbale/memo, con l'indicazione del nominativo e ruolo del rappresentante della Pubblica Amministrazione incontrato, dell'oggetto dell'incontro, ecc..;
- i funzionari della Pubblica Amministrazione devono essere accompagnati durante le verifiche ispettive da almeno due rappresentanti di TeamSystem;

- la documentazione deve essere conservata dal responsabile di direzione competente in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.
- tutta la documentazione deve essere verificata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- la gestione dei rapporti con i pubblici funzionari in caso di visite ispettive è totalmente nella responsabilità del responsabile di direzione competente, che gestisce i sopralluoghi dalla fase di accoglimento alla firma del verbale di accertamento;
- qualora i pubblici funzionari redigano un verbale in occasione degli accertamenti condotti presso la Società, il responsabile di direzione coinvolto ha l'obbligo di firmare questi verbali e di mantenerne copia nei propri uffici;
- devono essere previste specifiche attività di controllo gerarchico sulla documentazione da presentare per la richiesta di finanziamenti.
- Invio a cura dei Responsabili della Direzione/Area secondo le richieste dall'O.d.V. di un'analisi delle transazioni con la P.A. e delle indicazioni in merito all'effettivo rispetto delle procedure interne che governano le attività.

Formazione del Bilancio e adempimenti societari

- Le registrazioni contabili possono essere effettuate esclusivamente da soggetti abilitati nell'uso del sistema informatico adottato, in accordo ai livelli autorizzativi previsti dalla Società;
- Ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto; pertanto, è compito del dipendente a ciò incaricato, fare in modo che la documentazione di supporto sia facilmente reperibile e ordinata secondo criteri logici;
- Devono essere pianificate le attività necessarie alla chiusura dell'esercizio sociale e alla redazione del progetto di Bilancio secondo un calendario che deve essere comunicato a tutti i soggetti coinvolti nel processo;
- Deve essere identificato il personale preposto alla trasmissione della documentazione alla società di revisione;
- Il responsabile della società di revisione ha la facoltà di prendere contatto con gli O.d.V. della varie società del Gruppo per verificare congiuntamente situazioni che possano presentare aspetti di criticità in relazione alle ipotesi di reato considerate;
- Tutte le informazioni strumentali al processo valutativo o di stima delle voci di bilancio devono essere archiviate sotto la responsabilità delle Funzioni aziendali che producono/ricevono tali informazioni.
- Qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure correnti, deve essere previsto che la funzione preposta informi tempestivamente l'Organismo di Vigilanza;
- La bozza di bilancio deve essere sempre messa a disposizione degli Amministratori con ragionevole anticipo rispetto alla riunione del Consiglio di Amministrazione che approva il progetto di bilancio;

- Tutti i documenti contabili relativi agli argomenti indicati nell'ordine del giorno delle riunioni del Consiglio di Amministrazione devono essere completi e messi a disposizione degli Amministratori con ragionevole anticipo rispetto alla data della riunione;
- I documenti riguardanti la formazione delle decisioni che governano le operazioni delle attività a rischio sopra indicate, nonché quelli che danno attuazione alle decisioni devono essere archiviati e conservati a cura della funzione competente per l'operazione;
- L'accesso ai documenti già archiviati deve essere consentito solo alle persone autorizzate in base alle procedure operative aziendali, al Collegio Sindacale, alla Società di Revisione e all'Organismo di Vigilanza;
- La trasmissione delle informazioni deve essere consentita alle sole persone autorizzate e avvenire attraverso mezzi tecnici che garantiscano la sicurezza dei dati e la riservatezza delle informazioni;
- Ogni modifica ai dati contabili deve essere effettuata dalla sola Direzione/Funzione che li ha generati, garantendo la tracciabilità dell'operazione di modifica e previa formale autorizzazione del Direttore/Responsabile di Funzione;
- Per ciascuna funzione deve essere individuato un responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al Collegio Sindacale previa verifica della loro completezza, inerenza e correttezza;
- Le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal Collegio Sindacale, devono essere documentate e conservate a cura del responsabile di funzione;
- Tutti i documenti all'ordine del giorno delle riunioni dell'Assemblea o del Consiglio di Amministrazione relativi a operazioni sulle quali il Collegio Sindacale debba esprimere parere devono essere messi a disposizione di quest'ultimo con ragionevole anticipo rispetto alla data della riunione;
- Deve essere sempre garantita la tracciabilità di fonti e informazioni nei rapporti con il Soci e il Collegio Sindacale.

Gestione della Sicurezza sul lavoro

- Devono essere predisposti un budget, piani annuali e pluriennali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza;
- Devono essere definite procedure, ruoli e responsabilità in merito alle fasi dell'attività di predisposizione e attuazione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori;
- Devono essere definiti, in coerenza con le disposizioni di legge vigenti in materia, i meccanismi relativi a:
  - valutazione e controllo periodico dei requisiti di idoneità e professionalità del responsabile del servizio di prevenzione e protezione (c.d. "RSPP") e degli addetti al servizio di prevenzione e protezione (c.d. "ASPP");
  - definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;
  - processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza delle modalità e della tempistica in caso di avvicendamento nel ruolo;
- Devono essere definiti i meccanismi di predisposizione dei Documenti di Valutazione dei Rischi ("DVR", "DUVRI") per la Salute e la Sicurezza sul Lavoro;

- Deve essere predisposto un modello di monitoraggio sistemico e continuo dei dati/indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il sistema di prevenzione e protezione;
- Devono essere individuati i requisiti e le competenze specifiche per la conduzione delle attività di audit sul modello di Salute e Sicurezza dei lavoratori nonché le modalità e le tempistiche delle verifiche sullo stato di attuazione delle misure adottate;
- Devono essere previste riunioni periodiche con la dirigenza, con i lavoratori e i loro rappresentanti;
- Deve essere prevista la consultazione preventiva dei rappresentanti dei lavoratori in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
- Devono essere previsti meccanismi di controllo che garantiscano l'inclusione nei contratti di appalto, subappalto e somministrazione, dei costi relativi alla sicurezza del lavoro.

Gestione dei sistemi informativi

- Le attività di installazione e manutenzione degli applicativi sui pc possono essere eseguite solo dagli amministratori di sistema.
- I requisiti di autenticazione ai sistemi per l'accesso ai dati, alle applicazioni ed alla rete devono essere individuali ed univoci.
- Le regole per la creazione delle password di accesso alla rete, agli applicativi, e ai sistemi critici o sensibili devono essere chiaramente definite ed avere caratteristiche uniformi (ad esempio: lunghezza minima della password di 8 caratteri, uso di caratteri speciali, scadenza predefinita, ecc.).
- La gestione di account e di profili di accesso ai sistemi devono prevedere un iter formale di autorizzazione e registrazione dell'attribuzione, modifica e cancellazione; inoltre devono essere formalizzate procedure per l'assegnazione e l'utilizzo di privilegi speciali (amministratore di sistema/dei pc utenti, utenze di super user, ecc.).
- Verifiche periodiche dei profili utente al fine di convalidare il livello di responsabilità dei singoli con i privilegi concessi; i risultati devono essere opportunamente registrati.
- L'accesso fisico ai locali riservati in cui risiedono le infrastrutture IT è garantito mediante l'utilizzo di codici di accesso, token authenticator, pin, badge, valori biometrici; devono esser effettuati controlli periodici sulla corrispondenza delle abilitazioni concesse ed il ruolo ricoperto dall'utente autorizzato.
- A fronte di eventi disastrosi la Società deve prevedere un piano di Business Continuity ed un piano di Disaster Recovery, al fine di garantire la continuità dei sistemi informativi e dei processi ritenuti critici; le soluzioni individuate devono esser periodicamente aggiornate e testate;
- Gli accessi effettuati sugli applicativi dagli utenti devono essere oggetto di verifiche e, per quanto concerne l'ambito dei dati sensibili, le applicazioni devono tener traccia delle modifiche ai dati compiute dagli utenti e devono essere attivati controlli che identificano variazioni nei database aziendali;
- Devono essere condotte verifiche periodiche dei profili utente al fine di convalidare il livello di responsabilità dei singoli con i privilegi concessi; i risultati devono essere opportunamente registrati.
- La gestione dei sistemi hardware deve prevedere la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e regolamentare le responsabilità, le modalità operative in caso di implementazione e/o manutenzione di hardware in una procedura formalizzata.
- La gestione dei sistemi software deve includere la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione, sui principali sistemi, di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso;

- L'accesso fisico ai locali in cui risiedono le infrastrutture IT deve esser garantito mediante l'utilizzo di codici di accesso, pin e/o badge; devono esser effettuati controlli periodici sulla corrispondenza delle abilitazioni concesse ed il ruolo ricoperto dall'utente autorizzato.
- Deve essere implementato un sistema che preveda l'uso di tecniche crittografiche per la generazione, distribuzione, revoca ed archiviazione delle chiavi di cifratura;
- Devono esser predisposti ed opportunamente documentati i controlli per la protezione delle chiavi di cifratura da possibili modifiche, distruzioni, utilizzi non autorizzati.

Gestione degli adempimenti in materia ambientale

- Devono essere richieste e preventivamente acquisite tutte le autorizzazioni, nonché devono essere effettuate le comunicazioni necessarie alla gestione dei rifiuti;
- L'attività di gestione e smaltimento dei rifiuti deve essere svolta con la massima cura ed attenzione con particolare riferimento alla caratterizzazione dei rifiuti, alla gestione dei depositi temporanei, al divieto di miscelazione dei rifiuti siano essi pericolosi o non pericolosi;
- In sede di affidamento delle attività di smaltimento o recupero di rifiuti alle imprese autorizzate deve essere verificata: a) la data di validità dell'autorizzazione, b) la tipologia e la quantità di rifiuti per i quali è stata rilasciata l'autorizzazione ad esercitare attività di smaltimento o recupero; c) la localizzazione dell'impianto di smaltimento e d) il metodo di trattamento o recupero;
- In fase di esecuzione delle attività di trasporto di rifiuti da parte delle imprese autorizzate deve essere verificata: a) la data di validità dell'autorizzazione; b) la tipologia e la targa del mezzo; c) i codici CER autorizzati.

Progettazione e commercializzazione di prodotti

- Deve essere garantita la tracciabilità delle attività connesse allo sviluppo di nuovi prodotti e servizi;
- Nella fase di studio di fattibilità del progetto devono essere valutati possibili conflitti con titoli di proprietà industriale altrui;
- Deve essere assicurata la possibilità di ricostruire tutte le fasi che hanno portato allo sviluppo di un nuovo software
- I processi autorizzativi devono essere sempre accuratamente documentati e verificabili a posteriori;
- I rapporti con i clienti devono essere verificabili attraverso documentazione contrattuale completa e idonea a definire chiaramente ogni obbligo / diritto di entrambe le parti;
- Le controparti commerciali devono essere preventivamente verificate, attraverso le informazioni disponibili, , al fine di accertare la relativa rispettabilità e affidabilità prima di avviare rapporti d'affari, assicurando la tracciabilità degli accertamenti svolti.
- Le operazioni commerciali devono essere supportate da adeguata documentazione, secondo le modalità specifiche previste dalle procedure aziendali applicabili al processo in oggetto, e devono avvenire entro le linee guida stabilite dalla Società;
- Deve essere identificata una funzione responsabile della valutazione delle offerte nei contratti standard
- Deve essere effettuato un confronto tra il prezzo dell'offerta rispetto a quello di mercato e un eventuale passaggio autorizzativo in caso di scostamenti significativi;
- Deve essere assicurata una gestione controllata dell'emissione dell'ordine di vendita e delle successive eventuali modifiche.

Gestione delle informazioni privilegiate

- Devono essere definiti i ruoli e i compiti delle Funzioni e dei Responsabili coinvolti nella predisposizione e divulgazione di dati e notizie all'esterno e deve essere prevista la separazione tra la Funzione fornitrice dei dati, la Funzione incaricata della predisposizione del comunicato e la Funzione/Direzione che autorizza la diffusone dello stesso;
- Il soggetto responsabile dell'emissione dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni;
- È fatto divieto di diffondere l'informazione rilevante all'interno o all'esterno della Società, se non tramite il canale istituzionalmente previsto;
- Deve essere previsto un programma di informazione/formazione periodica di amministratori, management e dipendenti delle aree/funzioni aziendali a rischio sulla normativa in materia di abusi di mercato;
- Devono esistere procedure autorizzative per acquisti e vendite di strumenti finanziari propri e/o di altre società;
- Deve essere predisposto un Registro delle persone che hanno accesso alle informazioni privilegiate;
- Deve essere assicurata la riservatezza delle informazioni mediante l'adozione di confidenzialità volte a garantire la sicurezza organizzativa, fisica e logica delle informazioni privilegiate;
- Devono essere individuati i soggetti rilevanti e le operazioni da essi effettuate anche per interposta persona con riferimento agli strumenti finanziari della Società.

SEZIONE TERZA

3 Organismo di Vigilanza

3.1 L'Organismo di Vigilanza e i suoi requisiti

Al fine di garantire alla Società l'esimente dalla responsabilità amministrativa in conformità a quanto previsto dall'art. 6 del Decreto, è necessaria l'individuazione e la costituzione da parte della Società di un Organismo di Vigilanza fornito dell'autorità e dei poteri necessari per vigilare, in assoluta autonomia, sul funzionamento e sull'osservanza del Modello, nonché di curarne il relativo aggiornamento, proponendone le modifiche o integrazioni ritenute opportune al Consiglio di Amministrazione della Società.

I componenti dell'Organismo di Vigilanza della Società (di seguito anche "**OdV**") sono scelti tra soggetti in possesso dei requisiti di autonomia, indipendenza e professionalità richiesti dal Decreto per svolgere tale ruolo.

Il Decreto 231/01 non fornisce indicazioni alcuna circa la composizione dell'OdV; pertanto, la scelta tra una sua composizione monosoggettiva o plurisoggettiva e l'individuazione dei suoi componenti - interni o esterni all'ente - devono tenere conto - come suggerito dalle Linee Guida di Confindustria e come confermato dalla giurisprudenza in materia - delle finalità perseguite dalla legge in uno con la tipologia di società nella quale l'OdV andrà ad operare, dovendo esso assicurare il profilo di effettività dei controlli in relazione alla dimensione e alla complessità organizzativa dell'ente.

In base a tali indicazioni, l'OdV deve possedere le seguenti principali caratteristiche:

a) *Autonomia ed indipendenza*

I requisiti di autonomia ed indipendenza che l'OdV deve necessariamente possedere, affinché la Società possa andare esente da responsabilità, si riferiscono in particolare alla funzionalità dello stesso OdV. La posizione dell'OdV nell'ambito delle Società dovrà cioè assicurare l'autonomia dell'iniziativa di controllo da ogni interferenza o condizionamento proveniente dalla Società e dai suoi organi dirigenti. Tali requisiti sono assicurati tramite la collocazione dell'OdV in una posizione di vertice in seno all'organizzazione aziendale, senza attribuzione, formale o anche solo in via di fatto, di alcun ruolo esecutivo che possa renderlo partecipe di decisioni ed attività operative della Società, che altrimenti lo priverebbero della necessaria obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

I requisiti di autonomia e indipendenza oltre che a riferirsi all'OdV nel suo complesso debbono anche riferirsi ai suoi componenti singolarmente considerati: in caso di OdV a composizione plurisoggettiva, nei quali alcuni componenti siano esterni e altri interni, non essendo esigibile dai componenti di provenienza interna una totale indipendenza dalle Società, il grado di indipendenza dell'OdV dovrà essere valutato nella sua globalità.

Al fine di garantire l'effettiva sussistenza dei requisiti sopra descritti, è opportuno che i membri dell'OdV posseggano alcuni requisiti soggettivi formali che garantiscano ulteriormente la loro autonomia e indipendenza come previsto dalle Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231 approvate il 7 marzo 2002 ed aggiornate il marzo 2014 (ad esempio onorabilità, assenza di conflitti di interesse con gli organi sociali e con il vertice aziendale etc.).

b) *Professionalità*

I componenti l'OdV debbono possedere, così come specificato anche in talune pronunce giurisprudenziali, apposite competenze tecniche, onde poter provvedere efficacemente all'espletamento dei propri compiti ispettivi e di controllo. Trattasi di tecniche di tipo specialistico, proprie di chi svolge attività ispettiva, consulenziale e giuridica.

Con riferimento all'attività ispettiva e di analisi del sistema di controllo, è opportuno che i membri dell'OdV abbiano esperienza, ad esempio, nelle tecniche di analisi e valutazione dei rischi, nelle misure per il loro contenimento, nel *flow-charting* di procedure e processi per l'individuazione dei punti di debolezza, nelle tecniche di intervista e di elaborazione dei questionari.

Si ricorda in ogni caso che l'OdV, al fine di adempiere ai propri compiti, può utilizzare, oltre alle competenze specifiche dei singoli membri, anche risorse aziendali interne o consulenti esterni.

c) *Continuità di azione*

Al fine di garantire l'efficace e costante attuazione del Modello Organizzativo, l'OdV deve garantire continuità nell'esercizio delle sue funzioni, che non deve essere intesa come "presenza continua", ma come effettività e frequenza del controllo.

La definizione degli aspetti attinenti alla continuità d'azione dell'OdV, quali la calendarizzazione dell'attività, la verbalizzazione delle riunioni, la frequenza e la modalità delle riunioni, è rimessa allo stesso Organismo, il quale, nell'esercizio della propria facoltà di autoregolamentazione, dovrà disciplinare il proprio funzionamento interno. A tal proposito è opportuno che l'OdV stesso formuli un regolamento delle proprie attività (es. modalità di convocazione delle riunioni, documentazione dell'attività, etc.).

Si precisa, infine, che la Legge n. 183 del 2011 (c.d. Legge di Stabilità per il 2012), ha espressamente previsto la possibilità per le società di capitali di affidare al Collegio Sindacale le funzioni di Organismo di Vigilanza (art. 6, comma 4-bis del Decreto). Pertanto, la Società ha la facoltà di optare per questa forma di organizzazione dell'OdV, anche in considerazione delle esigenze di razionalizzazione complessiva del sistema dei controlli adottato.

3.2 Composizione dell'Organismo di Vigilanza, nomina, revoca, cause di ineleggibilità e di decadenza dei suoi membri

Il numero e la qualifica dei componenti dell'Organismo di Vigilanza è stabilito dal Consiglio di Amministrazione, che provvede alla nomina dell'OdV e del suo Presidente mediante apposita delibera consiliare motivata, che dia atto della sussistenza dei requisiti di autonomia, indipendenza e professionalità che i membri dell'OdV devono possedere.

I componenti dell'OdV rimangono in carica per tre anni e sono rieleggibili.

I componenti dell'Organismo di Vigilanza, nell'esercitare le proprie funzioni, devono mantenere i necessari requisiti di autonomia e indipendenza richiesti dal Decreto: essi devono pertanto comunicare immediatamente al Consiglio di Amministrazione e allo stesso Organismo di Vigilanza l'insorgere di eventuali situazioni che non consentano di conservare il rispetto di tali requisiti.

I membri dell'Organismo di Vigilanza designati restano in carica per tutta la durata del mandato ricevuto, a prescindere dalla modifica di composizione del Consiglio di Amministrazione che li ha nominati, a meno che il rinnovo del Consiglio di Amministrazione dipenda dalla commissione di uno dei Reati contemplati nel Decreto: in tal caso il neo eletto organo amministrativo provvederà a costituire un nuovo Organismo di Vigilanza.

Non possono essere eletti alla carica di componenti dell'Organismo di Vigilanza e, se eletti, decadono automaticamente dall'ufficio:

1. coloro che si trovano nelle condizioni previste dall'articolo 2382 del Codice Civile (interdizione, inabilitazione, fallimento, condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'incapacità ad esercitare uffici direttivi);

2. il coniuge, i parenti e gli affini entro il quarto grado degli amministratori non-indipendenti della Società; il coniuge, i parenti e gli affini entro il quarto grado degli amministratori non-indipendenti delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo;
3. coloro che sono stati condannati con sentenza ancorché non definitiva (ivi compresa quella pronunciata ex art. 444 c.p.p.):
   - alla reclusione per un tempo non inferiore a un anno: i) per uno dei delitti previsti dal RD n. 267/1942; ii) per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, dei mercati e dei valori mobiliari e di strumenti di pagamento; iii) per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica o in materia tributaria;
   - alla reclusione per un tempo non inferiore a due anni per qualunque delitto non colposo;
   - per uno o più reati tra quelli previsti e richiamati dal Decreto, a prescindere dal tipo di condanna inflitta;
   - per un reato che importi la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.
4. coloro nei cui confronti sia stata applicata una delle misure di prevenzione previste dall'art. 3 della legge 19 marzo 1990, n. 55 e sue successive modifiche.

In caso di nomina di un componente esterno, lo stesso non dovrà avere rapporti commerciali con la Società che possano determinare l'insorgere di conflitti di interesse.

Fatte salve le ipotesi di decadenza automatica, i componenti dell'OdV non possono essere revocati dal Consiglio di Amministrazione se non per giusta causa.

Rappresentano ipotesi di giusta causa di revoca:

- una sentenza di condanna della Società ai sensi del Decreto, o una sentenza di patteggiamento, ove risulti dagli atti l'"omessa o insufficiente vigilanza" da parte dell'OdV secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- il mancato riserbo relativamente alle informazioni di cui vengano a conoscenza nell'espletamento dell'incarico;
- la mancata partecipazione a più di due riunioni dell'OdV consecutive senza giustificato motivo.

In caso di dimissioni o di decadenza automatica di un componente dell'OdV, quest'ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione, che prenderà senza indugio le decisioni del caso.

L'OdV si intende decaduto se vengono a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, il Consiglio di Amministrazione provvede a nominare di nuovo tutti i componenti dell'OdV.

Ove sussistano gravi ragioni di convenienza, il Consiglio di Amministrazione procederà a disporre la sospensione dalle funzioni di uno o tutti i membri dell'OdV, provvedendo tempestivamente alla nomina di un nuovo membro o dell'intero Organismo ad interim.

3.3 L'Organismo di Vigilanza di Team System

Sulla base dei presupposti e delle considerazioni sopra riportate, contestualmente all'adozione del proprio Modello Organizzativo, la Società ha provveduto all'istituzione dell'Organismo di Vigilanza (OdV) e alla nomina dei suoi componenti. Nella sua attuale composizione, l'OdV è stato nominato con delibera del 16 marzo 2017.

La scelta è stata quella di affidare le funzioni di Organismo di Vigilanza ad un organismo a composizione collegiale, con un numero di membri pari a tre, individuati in due professionisti esterni, uno dei quali con

funzione di Presidente dell'OdV e in un componente interno i capo alla Direzione Affari societari, generali e legali di TeamSystem S.p.A..

In considerazione delle dimensioni e delle caratteristiche dell'organizzazione aziendale e della complessità dei compiti che l'OdV è chiamato a svolgere, la composizione sopra descritta pare la più idonea a garantire l'autonomia, la professionalità, nonché la continuità d'azione che devono contraddistinguere l'operato di detto Organismo.

La scelta di nominare due componenti esterni (individuando tra di essi il Presidente dell'OdV) risponde, invero, all'esigenza di rafforzare i requisiti di autonomia e indipendenza dell'Organismo, oltre che di professionalità dello stesso. Più precisamente, quale Presidente dell'OdV è stato individuato un professionista esterno, esercente la professione di avvocato, specializzato in diritto delle nuove tecnologie e dotato di competenze di carattere penalistico, oltre che specificatamente in materia di *compliance* al D.lgs. 231/2001. Quale ulteriore componente esterno è stato individuato un professionista revisore contabile, specializzato nelle attività di internal auditing, control e risk management.

Tutti i componenti hanno maturato esperienze professionali quali componenti di Organismi di vigilanza in società operanti a livello nazionale ed internazionale.

La presenza di un componente dell'Organismo di Vigilanza interno alla Società risponde, invece, all'esigenza di garantire la continuità d'azione dell'OdV nella concreta realtà aziendale, fornendo il necessario supporto alla gestione dei flussi informativi ed al coordinamento interno delle attività tra l'OdV e le unità organizzative aziendali e rafforzando il *committment* necessario ad un corretto esercizio dell'attività di vigilanza.

3.4 Compiti, Poteri e Funzioni dell'Organismo di Vigilanza

L'Organismo di Vigilanza svolge le funzioni di vigilanza e controllo previste dal Decreto e dal Modello.

L'Organismo di Vigilanza dispone di autonomi poteri di iniziativa e di controllo nell'ambito della Società tali da consentire l'efficace esercizio delle funzioni previste dal Decreto e dal Modello.

Per ogni esigenza necessaria al corretto svolgimento dei propri compiti, l'Organismo di Vigilanza dispone di adeguate risorse finanziarie che vengono assegnate allo stesso sulla base di *un budget* di spesa approvato dal Consiglio di Amministrazione, su proposta dell'OdV stesso. Le attività poste in essere dall'OdV non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che il Consiglio di Amministrazione è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto sul Consiglio di Amministrazione grava in ultima istanza la responsabilità del funzionamento e dell'efficacia del Modello.

L'OdV è chiamato a svolgere le seguenti attività:

i) ***Attività di verifica e vigilanza:***
- vigilanza sull'osservanza del Modello;
- verifica dell'effettiva adeguatezza e capacità del Modello di prevenire la commissione degli illeciti previsti dal Decreto;
- vigilanza sulla corretta applicazione del Sistema Disciplinare da parte delle funzioni aziendali allo stesso preposte;

ii) ***Aggiornamento del Modello***
- valutazione del mantenimento nel tempo della solidità e funzionalità del Modello, verificando che la Società curi l'aggiornamento del Modello e proponendo, se necessario, al Consiglio di Amministrazione o alle funzioni aziendali eventualmente competenti, l'adeguamento dello stesso, al fine di migliorarne l'adeguatezza e l'efficacia, in relazione alle mutate condizioni aziendali e/o legislative;
- attività di follow-up, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

iii) ***Informazione e formazione***

- promozione della diffusione nel contesto aziendale della conoscenza e della comprensione del Modello;
- promozione e monitoraggio delle iniziative, ivi inclusi i corsi e le comunicazioni, volte a favorire un'adeguata conoscenza del Modello da parte di tutti i Destinatari;
- valutazione e risposta alle richieste di chiarimento provenienti dalle funzioni aziendali ovvero dagli organi amministrativi e di controllo, qualora connesse e/o collegate al Modello.

iv) ***Reporting da e verso l'OdV***

- attuazione, in conformità al Modello, di un efficace flusso informativo nei confronti degli organi sociali competenti in merito all'efficacia e all'osservanza del Modello;
- verifica del puntuale adempimento, da parte dei soggetti interessati, di tutte le attività di *reporting* inerenti al Modello;
- esame e valutazione di tutte le informazioni e/o le segnalazioni ricevute in relazione al Modello, ivi incluso per ciò che attiene le eventuali violazioni dello stesso;
- in caso di controlli da parte di soggetti istituzionali, ivi inclusa la Pubblica Autorità, previsione del necessario supporto informativo agli organi ispettivi.

Nell'ambito delle attività sopra enunciate, l'OdV provvederà ai seguenti adempimenti:

- promuovere la diffusione e la verifica nel contesto aziendale della conoscenza e della comprensione dei principi delineati nel Modello;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree e le attività a rischio individuate, effettuando, qualora lo ritenga necessario ai fini dell'espletamento delle proprie funzioni, anche controlli non preventivamente programmati (c.d. "controlli a sorpresa");
- verificare e controllare la regolare tenuta ed efficacia di tutta la documentazione inerente le attività/operazioni individuate nel Modello;
- verificare periodicamente le procure e le deleghe interne in vigore, raccomandando le necessarie modifiche nel caso in cui le stesse non siano più coerenti con le responsabilità organizzative e gestionali;
- istituire (facendone richiesta alle competenti funzioni aziendali) specifici canali informativi "dedicati" (es. indirizzi di posta elettronica), diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- valutare periodicamente l'adeguatezza del Modello rispetto alle disposizioni ed ai principi regolatori del Decreto e le corrispondenti esigenze di aggiornamento;
- valutare periodicamente l'adeguatezza del flusso informativo e adottare le eventuali misure correttive;
- comunicare e relazionare periodicamente al Consiglio di Amministrazione in ordine alle attività svolte, alle segnalazioni ricevute, agli interventi correttivi e migliorativi del Modello e al loro stato di realizzazione.

Ai fini dello svolgimento degli adempimenti ad esso affidati, all'OdV sono attribuiti i poteri e le facoltà qui di seguito indicati

- emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'Organismo;
- accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'OdV, ivi inclusi i libri societari di cui all'art. 2421 del cod. civ.;
- richiedere la collaborazione, anche in via continuativa, di strutture interne o ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
- disporre che i soggetti destinatari della richiesta forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- condurre le indagini interne necessarie per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;

- richiedere alle funzioni aziendali preposte e delegate alla gestione dei procedimenti disciplinari e all'irrogazione delle sanzioni informazioni, dati e/o notizie utili a vigilare sulla corretta applicazione del sistema disciplinare;
- richiedere, attraverso i canali e le persone appropriate, la riunione del Consiglio di Amministrazione per affrontare questioni urgenti;
- accedere alla documentazione elaborata dal Collegio Sindacale;
- richiedere ai responsabili di funzione di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza.

Considerate le funzioni dell'Organismo di Vigilanza ed i contenuti professionali specifici da esse richieste, nello svolgimento dell'attività di vigilanza e controllo, l'Organismo di Vigilanza può avvalersi del supporto delle altre funzioni interne alla Società che, di volta in volta, si rendessero necessarie per un'efficace svolgimento delle attività di verifica.

L'Organismo di Vigilanza, qualora lo ritenga opportuno e/o nei casi in cui si richiedano a questa funzione attività che necessitino di specializzazioni professionali non presenti al suo interno, né all'interno della Società stessa, avrà la facoltà di avvalersi delle specifiche capacità professionali di consulenti esterni ai quali delegare predefiniti ambiti di indagine e le operazioni tecniche necessarie per lo svolgimento della funzione di controllo. I consulenti dovranno, in ogni caso, sempre riferire i risultati del loro operato all'Organismo di Vigilanza.

3.5 Reporting dell'Organismo di Vigilanza

L'OdV riferisce in merito all'attuazione del Modello ed all'attività svolta secondo le seguenti linee di *reporting:*

a) **su base annuale**, al Consiglio d'Amministrazione, al quale dovrà essere trasmessa una relazione scritta avente in particolare ad oggetto:
- l'attività complessivamente svolta nel periodo di riferimento;
- una *review* delle segnalazioni ricevute e delle azioni intraprese dall'OdV o da altri soggetti,
- ivi incluse le sanzioni disciplinari (connesse con comportamenti rilevanti ai fini del Decreto) eventualmente irrogate dai soggetti competenti;
- le criticità emerse in relazione al Modello ed i necessari e/o opportuni interventi correttivi e migliorativi del Modello e al loro stato di realizzazione;
- l'individuazione, con cadenza annuale, del piano di attività per l'anno successivo;
- lo stato di attuazione del Modello Organizzativo,

b) **su base continuativa e qualora ne ravvisi la necessità**, all'Amministratore Delegato e al Consiglio di Amministrazione. In particolare, l'OdV dovrà:
- segnalare tempestivamente al Consiglio di Amministrazione qualsiasi violazione del Modello che sia ritenuta fondata dall'Organismo stesso, di cui sia venuto a conoscenza per segnalazione da parte dei dipendenti o dallo stesso accertata;
- segnalare tempestivamente al Consiglio di Amministrazione rilevate carenze organizzative o procedurali idonee a determinare il concreto pericolo di commissione di reati rilevanti ai fini del Decreto;
- segnalare all'Amministratore Delegato o al Consiglio di Amministrazione l'esistenza di modifiche normative particolarmente rilevanti ai fini dell'attuazione ed efficacia del Modello;
- trasmettere tempestivamente al Consiglio d'Amministrazione ogni altra informazione rilevante al fine del corretto svolgimento delle funzioni proprie dell'Organismo stesso, nonché al fine del corretto adempimento delle disposizioni di cui al Decreto.

L'OdV di TeamSystem, potrà essere convocato in qualsiasi momento dai suddetti organi o potrà a sua volta presentare richiesta in tal senso, per riferire in merito al funzionamento del Modello o a situazioni specifiche.

3.6 Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza, secondo quanto previsto dai protocolli adottati e nelle singole Parti Speciali del Modello.

Per ciascuna "area a rischio reato" saranno identificati uno o più "Responsabili Interni" che dovranno, tra l'altro, fornire all'OdV i flussi informativi secondo le modalità e con la frequenza definite in uno specifico "Protocollo dei flussi informativi", che costituisce parte integrante del presente Modello Organizzativo. Si ritiene, infatti, opportuno che la gestione dei flussi informativi verso l'Organismo di Vigilanza sia regolata da una specifica procedura, opportunamente diffusa e comunicata a tutti i destinatari, allo scopo di assicurare una maggiore efficacia nell'attuazione dei flussi informativi. Anche nel caso in cui, nel periodo selezionato, non vi siano state segnalazioni significative da comunicare all'OdV, allo stesso dovrà essere inviata una segnalazione "negativa".

Sono stati inoltre istituiti precisi obblighi gravanti sugli organi sociali e sul personale di TeamSystem in particolare:

- gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello;
- i Destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni delle prescrizioni del Modello o fattispecie di reato.

Le segnalazioni di cui sopra devono essere effettuate in forma scritta al seguente indirizzo di posta elettronica:

organismodiviglianza@teamsystem.com

ovvero, a mezzo di posta, all'Organismo di Vigilanza presso la sede della Società, corrente in

TeamSystem S.p.A.
Att.ne Organo di Vigilanza
Via Sandro Pertini, 88
61121 - Pesaro

indicando sulla busta la dicitura "PERSONALE E STRETTAMENTE RISERVATO – DA NON APRIRE".

Fermo restando quanto precede, verranno esaminate, purché sufficientemente precise e circostanziate, anche le segnalazioni indirizzate o, comunque, portate a conoscenza dei singoli membri dell'Organismo di Vigilanza, i quali provvederanno a condividere le informazioni ricevute con gli altri componenti dell'Organismo.

L'Organismo di Vigilanza agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti, comunque, salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

In ogni caso, i flussi informativi trasmessi all'Organismo di Vigilanza devono necessariamente prevedere le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento della Società o di soggetti apicali, dai quali si evinca lo

svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;

- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- attività di controllo svolte dai responsabili di altre direzioni aziendali dalle quali siano emersi fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o del Modello;
- modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
- Procedimenti disciplinari avviati in relazione alla violazione del Codice Etico o del Modello Organizzativo e relativi esiti (anche in caso di archiviazione)
- segnalazione di infortuni gravi (in ogni caso qualsiasi infortunio con prognosi superiore ai 40 giorni) occorsi a dipendenti, addetti alla manutenzione, appaltatori e/o collaboratori presenti nei luoghi di lavoro della Società;
- eventuali ordini ricevuti dal superiore e ritenuti in contrasto con la legge, la normativa interna o il Modello;
- Elenco finanziamenti pubblici chiesti/ottenuti nel periodo con lo stato di avanzamento del progetto; Verbali di ispezioni, visite e accertamenti da parte di organi pubblici di vigilanza ed eventuali sanzioni;
- contenziosi attivi e passivi in corso e, alla loro conclusione, i relativi esiti;
- eventuali richieste o offerte di denaro, doni o di altre utilità provenienti da, pubblici ufficiali o incaricati di pubblico servizio;
- eventuali scostamenti significativi di *budget* o anomalie di spesa non debitamente motivati, emersi dalle richieste di autorizzazione nella fase di consuntivazione del Controllo di Gestione;
- eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- eventuali segnalazioni, non tempestivamente riscontrate dalle funzioni competenti, concernenti sia carenze o inadeguatezze dei luoghi, delle attrezzature di lavoro, ovvero dei dispositivi di protezione messi a disposizione della Società, sia ogni altra situazione di pericolo connesso alla tutela dell'ambiente e della salute e sicurezza sul lavoro.

3.7 Invio di informazioni sulle modifiche dell'organizzazione aziendale all'Organismo di Vigilanza

Al fine di agevolare le attività di verifica e monitoraggio svolte dall'Organismo di Vigilanza con riferimento alle attività a rischio di commissione reato ed alla luce dell'assetto organizzativo adottato dalla Società, i Responsabili Interni individuati in seno all'organizzazione aziendale quali referenti dell'Organismo di Vigilanza devono trasmettere all'Organismo di Vigilanza, ciascuno con riferimento alle attività svolte direttamente o comunque sotto la propria responsabilità, con la periodicità e secondo le modalità individuate dalla Società, anche su proposta dell'OdV, le seguenti informazioni:

- notizie relative a cambiamenti organizzativi (ad esempio, mutamenti negli organigrammi societari, revisioni delle procedure esistenti o adozioni di nuove procedure o *policies*, etc.);
- gli aggiornamenti e i mutamenti del sistema delle deleghe e dei poteri;
- le eventuali comunicazioni del soggetto incaricato della revisione legale dei conti riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni;
- copia dei verbali delle riunioni del Consiglio di Amministrazione e del Collegio Sindacale da cui emergano modifiche organizzative, criticità nell'attuazione del sistema di controllo interno o comunque fatti o notizie rilevanti ai fini della corretta attuazione o della necessità di aggiornamento del Modello Organizzativo;

- copia delle eventuali comunicazioni effettuate all'Autorità di Vigilanza (ad es: Autorità Garante per la Concorrenza e del mercato, Autorità garante per la protezione dei dati personali, etc.);
- ogni altra informazione che l'Organismo di Vigilanza dovesse richiedere l'esercizio delle sue funzioni.

3.8 Il regolamento dell'Organismo di Vigilanza

L'OdV ha la responsabilità di redigere un proprio regolamento interno volto a disciplinare gli aspetti e le modalità concrete dell'esercizio della propria azione, ivi incluso per ciò che attiene al relativo sistema organizzativo e di funzionamento.

3.9 Archiviazione delle informazioni

Di tutte le richieste, le consultazioni e le riunioni tra l'OdV e le altre funzioni aziendali, l'Organismo di Vigilanza ha l'obbligo di predisporre idonea evidenza documentale ovvero apposito verbale di riunione. Tale documentazione verrà custodita sotto la responsabilità dell'Organismo di Vigilanza medesimo.

Ogni informazione, segnalazione, report previsti dal presente Modello sono conservati dall'Organismo di Vigilanza in un apposito e riservato archivio informatico e/o cartaceo in conformità alle disposizioni contenute nel Decreto n. 196/2003 e per un periodo di 10 anni.

SEZIONE QUARTA

4 Sistema sanzionatorio

4.1 Destinatari e apparato sanzionatorio e/o risolutivo

Aspetto essenziale per l'effettività del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al Decreto, e, in generale, delle procedure interne previste dal Modello stesso.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.

Sanzioni per i lavoratori dipendenti

Ai comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono applicabili – fatta eccezione per i richiami verbali – le procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e le norme pattizie di cui al Contratto Collettivo Nazionale di Lavoro del Commercio a cui si rimanda.

In particolare, in caso di (a) violazione delle disposizioni del Modello, delle sue procedure interne (ad esempio il mancato rispetto delle procedure, la mancata comunicazione delle informazioni richieste all'Organismo di Vigilanza, il mancato svolgimento dei controlli, etc.), del Codice Etico, del Decreto o di qualsivoglia altra disposizione penale in esso inclusa o (b) mancato rispetto delle disposizioni di cui al Modello nello svolgimento di attività in aree "a rischio" o (c) danneggiamento della Società o l'aver causato una situazione oggettiva di pericolo per i beni della stessa (gli "Illeciti Disciplinari") saranno applicabili i seguenti provvedimenti disciplinari per i Dipendenti:

- richiamo verbale;
- ammonizione scritta;
- multa in misura non eccedente l'importo di 4 ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di 10 giorni;
- licenziamento.

Sanzioni nei confronti dei dirigenti

Nel caso in cui i dirigenti commettano un Illecito Disciplinare, si provvederà ad applicare nei confronti dei responsabili le seguenti misure in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti industriali:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel richiamo scritto all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave violazione – o ripetute violazioni - di una o più prescrizioni del Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del licenziamento con preavviso;
- laddove la violazione di una o più prescrizioni del Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il lavoratore incorre nel provvedimento del licenziamento senza preavviso.

Sanzioni nei confronti dei membri dell OdV

In caso di Illeciti Disciplinari commessi da membri dell'OdV, il Consiglio di Amministrazione dovrà essere prontamente informato e lo stesso potrà richiamare per iscritto tale membro dell'OdV o revocarlo a seconda della gravità dell'illecito commesso. Le sanzioni previste per dipendenti e dirigenti si applicheranno altresì ai membri dell'OdV che ricadono in tali categorie.

Misure nei confronti degli Amministratori e dei Sindaci

In caso di Illeciti Disciplinari commessi da Amministratori o da Sindaci della Società, l'OdV informerà l'intero Consiglio di Amministrazione e il Collegio Sindacale della stessa i quali provvederanno ad assumere le opportune iniziative previste dalla vigente normativa, coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, revoca per giusta causa, ecc.).

Misure nei confronti di Collaboratori, Partner e Consulenti

I Collaboratori esterni, fornitori, i Consulenti e i Partner della Società, con particolare riferimento a soggetti coinvolti nella prestazione di attività, forniture o servizi che interessano attività a rischio ai sensi del Modello, vengono informati sull'adozione del Modello e dell'esigenza della Società, che il loro comportamento sia conforme ai principi di condotta ivi stabiliti.

La Società valuta le modalità (ad es. diffusione sul sito Intranet), a seconda delle diverse tipologie di collaboratori esterni e partner, con cui provvedere ad informare tali soggetti sulle politiche e sulle procedure seguite dalla Società in virtù dell'adozione del Modello e per assicurarsi che tali soggetti si attengono al rispetto di tali principi, prevedendo altresì l'adozione di idonee clausole contrattuali che obblighino tali soggetti ad ottemperare alle disposizioni del Modello medesimo, sotto pena di risoluzione automatica del rapporto contrattuale e fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società.

5 Aggiornamento del Modello

L'adozione e l'efficace attuazione del Modello sono - per espressa previsione legislativa - una responsabilità rimessa al Consiglio di Amministrazione. Ne deriva che il potere di adottare eventuali aggiornamenti del Modello compete, dunque, al Consiglio di Amministrazione, che lo eserciterà mediante delibera con le modalità previste per la sua adozione.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal Decreto.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione.

A tal riguardo, si ricorda che il Decreto espressamente prevede la necessità di aggiornare il Modello al fine di renderlo costantemente "ritagliato" sulle specifiche esigenze dell'ente e della sua concreta operatività. Gli interventi di adeguamento e/o aggiornamento del Modello potranno rendersi ad esempio necessari in occasione di:

- innovazioni normative;

- violazioni del Modello e/o rilievi emersi nel corso di verifiche sull'efficacia del medesimo (che potranno anche essere desunti da esperienze riguardanti altre società);
- modifiche della struttura organizzativa dell'ente, anche derivanti da operazioni di finanza straordinaria ovvero da mutamenti nella strategia d'impresa derivanti da nuovi campi di attività intrapresi.

6 Informazione e formazione del personale

Obiettivo della Società è una pronta e puntuale diffusione dei contenuti del presente documento e del Modello agli amministratori, dirigenti, dipendenti della Società ed a tutti coloro che collaborino con essa.

In tale contesto:

I. ***Comunicazione iniziale e informazione***: l'adozione del Modello viene comunicata ai dipendenti, ai responsabili di funzione e ai dirigenti attraverso:

- l'invio di una comunicazione a firma dell'Amministratore Delegato a tutto il personale sui contenuti del Decreto, l'importanza dell'effettiva attuazione del Modello, le modalità di informazione previste dalla Società;
- la messa a disposizione del Modello nelle modalità più idonee, tra cui: i) la consegna di copia dello stesso nelle sessioni di formazione; ii) idonea diffusione sul sito intranet e internet; iii) l'affissione in bacheca; iv) l'invio dello stesso in formato elettronico;

II. ***Formazione***: È inoltre prevista un'adeguata attività formativa del personale e dei collaboratori della Società sui contenuti del Decreto e del Modello***.*** Tale attività formativa viene articolata nelle seguenti fasi:

- attività di formazione generale: i.e. un'attività di formazione generica volta ad informare i destinatari sulle prescrizioni del Decreto e sui contenuti del Modello adottato dalla Società;
- attività di formazione specifica: i.e. un'attività di formazione specifica di coloro che operano nella aree a rischio reato volta ad informare i destinatari, in particolare sui a) i rischi specifici a cui è esposta l'area nella quale operano e b) i principi di condotta e le procedure aziendali che essi devono seguire nello svolgimento della loro attività. La formazione, in particolare, dovrà riguardare, oltre al Codice Etico, anche gli altri strumenti di prevenzione quali le procedure, le policies, i flussi di informazione e gli altri protocolli adottati dalla Società in relazione alle diverse attività a rischio.

L'attività formativa è organizzata tenendo in considerazione, nei contenuti e nelle modalità di erogazione, della qualifica dei destinatari e del livello di rischio dell'area in cui operano e potrà, dunque, prevedere diversi livelli di approfondimento, con particolare attenzione verso quei dipendenti che operano nelle aree a rischio.

I corsi di formazione, le relative tempistiche e le modalità attuative saranno definite dal responsabile delle Risorse Umane sentito il parere dell'OdV, che provvederanno anche a definire le forme di controllo sulla frequenza ai corsi e la qualità del contenuto dei programmi di formazione. In particolare, la formazione potrà essere realizzata mediante sessioni in aula, in modalità e-learning e con la consegna di materiale informativo volto ad illustrare i contenuti del Decreto, il Modello Organizzativo e le sue componenti (ivi incluso il Codice Etico ed il Sistema Disciplinare).

La partecipazione ai corsi di formazione sul Modello è obbligatoria; la mancata partecipazione alle attività di formazione costituisce una violazione del Modello stesso e può dar luogo all'applicazione di sanzioni disciplinari.

Sono previste, inoltre, forme di verifica dell'apprendimento da parte dei destinatari della formazione mediante questionari di comprensione dei concetti esposti durante le sessioni formative, con obbligo di ripetizione della formazione in caso di esito non soddisfacente.

Il sistema di informazione e formazione è costantemente verificato e, ove occorra, modificato dall'OdV, in collaborazione con la Direzione Risorse Umane o di altri responsabili di funzione.

L'attività di informazione e formazione effettivamente svolta dovrà essere opportunamente documentata e la relativa documentazione sarà conservata dalla Direzione delle Risorse Umane.

PARTE SPECIALE "A" – REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

A.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)

Per quanto concerne la presente Parte Speciale "A", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati negli artt. 24 e 25 del Decreto e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere tout court, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). Tenuto conto che il momento del consumo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)

Tale ipotesi di reato si configura 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 dall'Unione europea. In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

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

Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da uno a cinque anni

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

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per omettere o ritardare o per aver omesso o ritardato atti del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà altresì estrinsecarsi in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara). Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Circostanze aggravanti (art. 319-bis c.p.)

La pena è aumentata se il fatto di cui all´articolo 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l´amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi.

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

Tale ipotesi di reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p. sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Il reato di corruzione in atti giudiziari può essere commesso nei confronti di giudici o membri del Collegio Arbitrale competenti a giudicare

sul contenzioso/arbitrato nell'interesse dell'Ente (compresi gli ausiliari e i periti d'ufficio), e/o di rappresentanti della Pubblica Amministrazione, quando questa sia una parte nel contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli.

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

Tale ipotesi di reato punisce la condotta dei soggetti apicali o dei soggetti subordinati che siano indotti a versare o promettere denaro o altra utilità, in ragione dell'abuso di potere del pubblico ufficiale o dell'incaricato di pubblico servizio.

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

La norma estende l'applicabilità degli artt. 318 e 319 anche all'incaricato di un pubblico servizio.

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

Le pene stabilite nel primo comma dell'articolo 318, nell'art. 319, nell'art. 319-bis, nell'articolo 319-ter e nell'art. 320 c.p. in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.

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

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio per l'esercizio delle sue funzioni, per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri e tale offerta o promessa non sia accettata.

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.)

La fattispecie prevede un reato comune che può essere commesso da chiunque. Il fatto che costituisce reato consiste nel procurare a sé o ad altri un ingiusto profitto a danno di un'altra persona (in questa fattispecie il danno deve essere subito dello Stato o da altro ente pubblico), inducendo, mediante artifici o raggiri, taluno in errore. Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

E' opportuno notare che il reato di cui all'art. 640-bis assume carattere generale, rispetto a quello previsto e punito dall'art. 316-ter che assume invece carattere sussidiario. Inoltre il reato in questione può facilmente concorrere con quello di cui all'art. 316-bis, in quanto può concretizzare condotte prodromiche all'erogazione del contributo distratto dalla destinazione prevista.

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del Decreto stesso, nell'ipotesi in cui un Dipendente od un Agente della Società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).

Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

Le disposizioni degli articoli 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

La fattispecie in esame è diretta a reprimere le ipotesi di illecito arricchimento conseguito alterando in qualunque modo il funzionamento di un sistema informatico o telematico, condotta integrata quando si attui una interferenza con il regolare svolgimento di un processo di elaborazione dati al fine di ottenere uno spostamento patrimoniale ingiustificato. Altra modalità di realizzazione del reato consiste nell'intervento abusivo su dati, programmi o informazioni contenuti in un sistema informatico o telematico, intervento attraverso il quale l'agente procura a sé o ad altri un ingiusto profitto con danno altrui. Da notare che la fattispecie in esame viene presa in considerazione dal Decreto soltanto nell'ipotesi in cui il fatto sia commesso in danno dello Stato o di altro Ente Pubblico.

A.2 Aree a rischio

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato e tale da ricomprendere anche la Pubblica Amministrazione di Stati esteri). Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte speciale "A", sono:

- Partecipazione a bandi per assegnazione di pubbliche forniture
- Gestione dei rapporti con la Pubblica Amministrazione nel caso di vittoria di un bando di gara e di eventuali contenziosi giudiziali e stragiudiziali relativi all'esecuzione di tali rapporti
- Gestione dei rapporti di "alto profilo" con soggetti appartenenti alla Pubblica Amministrazione

- Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti Pubblici di rilevanza nazionale e locale (es. Ministeri, Enti Locali Territoriali, a titolo di esempio Province e Comuni).

- Gestione degli adempimenti, delle comunicazioni e delle richieste, anche in occasione di verifiche, ispezioni ed accertamenti da parte degli enti pubblici competenti o delle autorità amministrative indipendenti
  - Gestione di rapporti con i Funzionari pubblici e adempimenti presso enti istituzionali competenti, quali ad es.
    - ✓ rapporti con i funzionari della Guardia di Finanza, dell'Agenzia delle Entrate e degli Enti competenti in materia fiscale, tributaria anche in occasione di verifiche, ispezioni e accertamenti;
    - ✓ adempimenti presso l'Ufficio Brevetti del Ministero dello Sviluppo Economico per l'espletamento delle attività previste nell'ambito della domanda di brevetto per un software elaborato dalla Società.
  - Rapporti con le Autorità Amministrative Indipendenti (es. Autorità Garante della Concorrenza e del mercato) e gestione delle comunicazioni e delle informazioni a esse dirette, anche in occasione di verifiche ispettive.

- Gestione dei rapporti con gli enti pubblici competenti per l'espletamento degli adempimenti necessari alla richiesta di finanziamenti e contributi, e predisposizione della relativa documentazione
  - Gestione dei rapporti con Funzionari degli Enti Pubblici finanziatori, internazionali, nazionali e locali (es. Comunità Europea, Regione, Provincia), per il conseguimento, a titolo esemplificativo, di finanziamenti, anche a fondo perduto, contributi o erogazioni pubbliche finalizzati alla realizzazione di progetti di formazione in sede di:
    - ✓ ottenimento delle informazioni connesse ai bandi di gara;
    - ✓ presentazione della richiesta;
    - ✓ verifiche e accertamenti circa il corretto utilizzo del finanziamento.
  - Predisposizione e trasmissione della documentazione per la richiesta del finanziamento (es. documentazione amministrativa richiesta dal bando, documentazione tecnica, etc.) e/o della documentazione di rendicontazione.
  - Gestione del finanziamento in termini di modalità di utilizzo dello stesso.

- Gestione degli adempimenti in materia di assunzioni, cessazione del rapporto di lavoro, retribuzioni, ritenute fiscali e contributi previdenziali e assistenziali, relativi a dipendenti e collaboratori
  - Gestione dei rapporti con i Funzionari Pubblici in occasione di verifiche circa il rispetto dei presupposti e delle condizioni (ad es. piano formativo, durata, rispetto dei limiti d'età, ecc.) richieste dalla normativa vigente per le assunzioni agevolate.
  - Gestione dei rapporti, anche tramite consulenti esterni, con funzionari competenti (INPS, INAIL, ASL, Direzione Provinciale del Lavoro ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento, anche in occasione di verifiche ispettive:
    - ✓ predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro;
    - ✓ autorizzazione per l'assunzione di personale appartenente a categorie protette;

- ✓ elenchi del personale attivo, assunto e cessato presso l'INAIL;
- ✓ controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente.

- Gestione dei contenziosi (es.: civili, tributari, giuslavoristici, amministrativi, penali), in tutti i gradi di giudizio
  - Gestione dei rapporti con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi (civile, penale, amministrativo, giuslavoristico e tributario) con particolare riferimento alla nomina dei legali esterni.

- Gestione degli adempimenti in materia societaria
  - Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. Registro delle imprese presso le Camere di Commercio competenti).

- Gestione delle partnership
  - Gestione dei rapporti con società pubbliche e private con le quali si intende stipulare accordi di partnership, con particolare riferimento alle seguenti attività:
    - ✓ individuazione delle opportunità di partnership commerciali/tecnologiche;
    - ✓ definizione degli accordi con i Partner.

- Gestione del sistema sicurezza ai sensi del D.Lgs. 81/08 (Testo Unico Sicurezza)
  - Gestione dei rapporti con le autorità in materia di tutela della sicurezza e salute sul lavoro, anche in occasione di verifiche e ispezioni, in occasione di, a titolo esemplificativo:
    - ✓ adempimenti previsti dal D.lgs. 81/2008 – Testo Unico sulla Sicurezza nei luoghi di lavoro;
    - ✓ relative ispezioni in materia di sicurezza, salute, igiene sul lavoro;
    - ✓ ottenimento del Certificato Prevenzione Incendi;
    - ✓ autorizzazione sanitaria.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

A.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

La presente Parte Speciale, prevede l'espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventare tali;
- porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi dei reati previsti nel Decreto ed in particolare sono tenuti a osservare, oltre ai principi generali enunciati nella Parte Generale (cfr. 2.10), i seguenti principi:

- stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione;
- instaurazione e mantenimento di qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza;
- instaurazione e mantenimento di qualsiasi rapporto con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e l'imparzialità nello svolgimento degli stessi.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

- effettuare ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia a pubblici funzionari;
- assecondare la condotta induttiva del Funzionario Pubblico, corrispondendo o promettendo denaro o altra indebita utilità per evitare un danno o conseguire un vantaggio illecito.
- distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte), o la brand image della Società. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto;
- effettuare prestazioni in favore dei consulenti, dei Partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
- presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;

- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- nei rapporti con interlocutori appartenenti alla Pubblica Amministrazione è fatto divieto di effettuare spese di rappresentanze (rimborso viaggi, soggiorni ecc.) ingiustificate;
- inoltre, nei confronti della Pubblica Amministrazione è fatto espresso divieto di:
    - esibire documenti e dati incompleti e/o comunicare dati falsi e alterati;
    - sottrarre o omettere l'esibizione di documenti veri;
    - omettere informazioni dovute;
- nel corso dei processi civili, penali o amministrativi, è fatto divieto di porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa;
- in particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di elargire, promettere o dare denaro o altra utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni, ecc.., ovvero a persone comunque indicate da codesti soggetti, nonché adottare comportamenti – anche a mezzo di soggetti terzi (es. professionisti esterni) - contrari alla legge e ai presidi aziendali, per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della Pubblica Amministrazione, quando questa sia una parte nel contenzioso;
- è altresì fatto divieto di favorire indebitamente gli interessi della Società inducendo con violenza o minaccia, o, alternativamente, con offerta di danaro o altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale.

A.4 Responsabile interno

Per ogni area a rischio, come individuate al punto A.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno")

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

A.5 Processi strumentali e sistema di controllo

Di seguito sono riportati i processi c.d. strumentali/funzionali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Consulenze e incarichi professionali a terzi
- Acquisto di beni e servizi
- Rimborsi spese, anticipi e spese di rappresentanza
- Flussi monetari e finanziari
- Gestione del contenzioso
- Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità
- Selezione, assunzione, gestione del personale dipendente
- Rapporti con la Pubblica Amministrazione
- Gestione delle informazioni privilegiate

La dettagliata individuazione del sistema dei controlli interni adottato dalla Società per la prevenzione dei Reati in questione (comprensivo, tra l'altro, di regole di comportamento, policy e procedure aziendali, strumenti di tracciabilità e di organizzazione) è contenuta nella documentazione di Risk Assessment redatta preliminarmente all'adozione del Modello Organizzativo. Peraltro, anche successivamente all'esecuzione del Risk Assessment, la Società ha provveduto ad integrare ed ampliare il proprio sistema di controllo per la prevenzione dei Reati contro la PA, attraverso l'implementazione di una serie di azioni di miglioramento dirette a garantire l'effettiva idoneità ed il costante aggiornamento nel tempo del Modello Organizzativo.

I protocolli per la prevenzione dei Reati contro la PA sono costituiti, pertanto, dall'insieme di tali strumenti, nonché dai principi di comportamento e dalle prescrizioni di cui alla presente Parte Speciale. Inoltre, a titolo esemplificativo e non esaustivo, la Società è dotata dei seguenti strumenti specifici di controllo e prevenzione in relazione alle Aree a rischio sopra considerate:

- Approvvigionamento beni e servizi (ciclo passivo)
- Manuale di qualificazione dei fornitori
- Gestione omaggi
- Gestione sponsorizzazioni ed erogazioni liberali
- Formazione del Bilancio di esercizio, consolidato e delle situazioni contabili infrannuali, gestione degli adempimenti societari, gestione dei rapporti con gli Organi sociali e di controllo
- Procedura di gestione del contenzioso
- Procedura di gestione delle risorse umane
- Procedura di gestione dei rapporti con la Pubblica Amministrazione
- Policy rimborsi spese e trasferte
- Procedura gestione crediti di Gruppo
- Procedura di gestione della tesoreria e dei flussi monetari e finanziari

PARTE SPECIALE "B" - REATI SOCIETARI

B.1 Le tipologie dei reati societari (art. 25-ter del Decreto)

Per quanto concerne la presente Parte Speciale "B", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati e indicati all'art. 25-ter del Decreto (di seguito i "Reati Societari) e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico della Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

False comunicazioni sociali (articolo 2621 del codice civile), Fatti di lieve entità (articolo 2621-bis del codice civile) e False comunicazioni sociali delle società quotate (articolo 2622 del codice civile) .
I reati di false comunicazioni sociali sono stati profondamente riformati con la L. 27 maggio 2015, n. 69. In particolare, il reato di false comunicazioni sociali sia in società quotate (o ad esse equiparate), che in società non quotate, si realizza tramite la consapevole esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali rilevanti non rispondenti al vero, ovvero tramite la consapevole omissione di fatti materiali rilevanti sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene con l'intenzione di ingannare i soci o il pubblico, la cui comunicazione è imposta dalla legge.
Si precisa che:

- soggetti attivi del reato possono essere amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori (trattasi, quindi, di cd. "reato proprio"), nonché coloro che secondo l'articolo 110 del codice penale concorrono nel reato da questi ultimi commesso;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- la condotta deve essere concretamente idonea ad indurre in errore i destinatari delle comunicazioni imposte dalla legge;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Rispetto alla previgente formulazione delle norme in esame, la Legge 69/2015 ha eliminato le soglie di punibilità che prima limitavano in modo consistente la possibilità di imputare il reato al soggetto agente e di introdurre invece, per le società non quotate o ad esse equiparate, la definizione di fatti di lieve entità (art. 2621-*bis*, c.c.) e di particolare tenuità (art. 2621-*ter*, c.c.) per i quali si applica rispettivamente una pena meno grave e una causa di esclusione della punibilità. Infatti, mentre per le società quotate (o ad esse equiparate) non sono previste specifiche attenuanti, per le società non quotate, con l'introduzione dell'art. 2621-*bis* c.c., si è previsto che la pena possa essere ridotta (da sei mesi a tre anni) nel caso in cui gli illeciti siano di "lieve entità", tenuto conto sia della natura e delle dimensioni della società, sia delle modalità o degli effetti della condotta. Con riferimento alle società non soggette a fallimento, il legislatore ha introdotto una presunzione per la quale la condotta dell'agente in questo tipo di società debba essere sempre considerata di lieve entità, in tal caso il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale. Con l'introduzione dell'art. 2621-*ter* c.c. si individua l'ulteriore fattispecie della non punibilità per "particolare tenuità" di cui al nuovo art. 131-*bis* c.p., precisando che detta qualificazione dovrà essere oggetto di accertamento da parte del giudice, chiamato a valutare ("in modo prevalente") l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori conseguente ai fatti di cui agli artt. 2621 e 2621-*bis* c.c.
Inoltre, la Legge 69/2015 ha ricondotto le false comunicazioni sociali, precedentemente configurate dall'art. 2621 c.c. quali reati contravvenzionali e illeciti amministrativi, al novero dei delitti, punibili con la pena della reclusione.
E' da rilevare, infine, come le modifiche al falso in bilancio abbiano impattato sulla disciplina del d.lgs. 231/2001 non solo per quanto riguarda l'indicazione dei reati presupposto (ai quali oggi si aggiunge, oltre ai riformulati articoli 2621 e 2622, anche l'art. 2621-*bis*, c.c.) ma anche per quanto concerne l'ambito applicativo della

disposizione dell'art. 25-*ter* del decreto che, nella formulazione previgente, restringeva il novero ai reati societari commessi nell'interesse della società da amministratori, direttori generali o liquidatori, ovvero da persone sottoposte alla loro vigilanza, laddove la realizzazione del fatto fosse imputabile ad una violazione dei doveri di vigilanza imposti dagli obblighi inerenti la loro carica. Il nuovo testo dell'art. 25-*ter*, come modificato dalla L. 69/2015, si limita invece a disporre l'applicazione delle sanzioni pecuniarie "*in relazione ai reati in materia societaria previsti dal codice civile*", stabilendone l'entità, con l'eliminazione di qualsiasi riferimento alla nozione di "interesse" della società, al novero dei soggetti dalle cui azioni possono derivare le conseguenze sanzionatorie per l'ente e, infine, ai criteri di imputazione oggettiva dell'illecito.
Con riferimento alle pene previste per il reato di falso in bilancio, la Legge 69/2015 ha previsto che, nei confronti dell'ente, trovino applicazione le seguenti sanzioni pecuniarie:

- da 200 a 400 quote per il delitto di false comunicazioni sociali ex art 2621 c.c. (quindi da un minimo di euro 51.644 ad un massimo di euro 619.748;
- da 100 a 200 quote per il delitto di false comunicazioni sociali ex art 2621-bis c.c. (quindi da un minimo di euro 25.822 ad un massimo di euro 309.874);
  da 400 a 600 quote per il delitto di false comunicazioni sociali ex art. 2622 c.c. (quindi da un minimo di euro 103.288 ad un massimo di euro 929.622).

Impedito controllo (art. 2625 c.c.)

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali qualora tale condotta abbia cagionato un danno ai soci.

L'illecito può essere commesso esclusivamente dagli amministratori.

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

Tale ipotesi di reato consiste nel procedere, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.

Soggetti attivi del reato possono essere solo gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art.110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

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

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di 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.

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art.110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori.

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

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

Tale ipotesi di reato è integrata dalle seguenti condotte: a) formazione o aumento in modo fittizio del capitale sociale mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; b) sottoscrizione reciproca di azioni o quote; c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti.
Si precisa che non è, invece, incriminato l'omesso controllo ed eventuale revisione da parte di amministratori e sindaci, ai sensi dell'art. 2343, 3° comma, c.c. della valutazione dei conferimenti in natura contenuta nella relazione di stima redatta dall'esperto nominato dal Tribunale.

Corruzione tra privati (2635 c.c.)

Tale ipotesi di reato è stata riformata con il D.Lgs. 38/2017. L'attuale formulazione della norma prevede che gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per se' o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni.

L'art. 2635 co. 1 prevede che la stessa pena si applica lai fatti commessi da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo; mentre, qualora il fatto sia commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei predetti soggetti, la pena sarà fino a un anno e sei mesi di reclusione.

Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste (art. 2635 co. 3 c.c.). Si fa presente che l'ente risponderà solo in quest'ultimo caso, cioè quando i predetti soggetti agiscono in qualità di corruttori, e non anche nei casi in cui siano stati corrotti.

Si noti infine che l'art. 2635 c.c., unitamente al successivo art. 2635-bis c.c., rappresentano gli unici reati societari per i quali, oltre alla sanzione pecuniaria, a carico dell'ente è prevista anche la sanzione interdittiva.

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

La norma è stata introdotta con il D.Lgs. 38/2017 per i fatti commessi successivamente al 14 aprile 2017.

Il primo comma punisce chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata. Tale fattispecie è astrattamente idonea a coinvolgere la responsabilità amministrativa dell'ente.

Per completezza, pur non avendo rilievo ai fini della responsabilità amministrativa dell'ente, si evidenzia che allo stesso modo sono puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti privati nonché coloro che svolgono in essi un'attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri -anche per interposta persona- una promossa o una dazione di denaro o altra utilità per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, nei casi in cui la sollecitazione non sia accettata.

Unitamente alla fattispecie prevista dall'art. 2635 co. 3 c.c., la fattispecie prevista al primo comma dell'art. 2635-bis c.c. rappresenta l'unica ipotesi di reato societario per il quale oltre alla sanzione pecuniaria, a carico dell'ente è prevista anche la sanzione interdittiva.

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

Si tratta di due ipotesi di reato distinte per modalità di condotta e momento offensivo:

- la prima si realizza (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità pubbliche di Vigilanza (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria. La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti od amministrati dalla società per conto di terzi;
- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche Autorità, attuato consapevolmente e in qualsiasi forma, anche omettendo le comunicazioni dovute alle Autorità medesime.

Il termine "Autorità pubblica di Vigilanza" (letteralmente, "autorità di vigilanza") è chiaramente generico, completamente indeterminato e fa sorgere rilevanti dubbi interpretativi. In maniera precauzionale il termine è stato interpretato in maniera tale da includere tutte le autorità amministrative esistenti nel nostro sistema giuridico senza considerare il tipo di vigilanza concretamente svolto dalle stesse e l'indipendenza dal potere politico: pertanto, l'autorità garante per la protezione dei dati personali (così come l'autorità garante della concorrenza e del mercato e l'autorità per la garanzia nelle comunicazioni) può essere considerata autorità di vigilanza, l'esercizio delle funzioni di tali autorità è tutelato dal dettato normativo dell'articolo 2638 c.c.

Dato quanto sopra, il reato di cui all'articolo 2638 c.c. deve essere riferito a specifiche e determinate tipologie di informazione, che possono attenere alla posizione economica e finanziaria del soggetto sottoposto alla vigilanza dell'autorità in questione. Tale requisito richiesto espresso dalla legge limita la sua applicazione e richiede di riflettere sulla tipologia di dati e informazioni che nel caso specifico verranno comunicati all'autorità di vigilanza, il reato di realizza solo quando l'informazione comunicata ha le caratteristiche previste dalla legge.

Considerazioni analoghe devono essere fatte con riferimento ai rapporti della Società con le altre autorità di vigilanza.

Soggetti attivi dell'ipotesi di reato descritta sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

I reati la cui commissione è stata ritenuta remota sono i seguenti:

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

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto od alla sottoscrizione di azioni o quote emesse dalla società (o dalla 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.

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

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

Tale ipotesi di reato consiste nella violazione degli obblighi previsti dall'art. 2391, comma primo, c. c. da parte dell'amministratore di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione Europea o diffusi fra il pubblico in maniera rilevante ai sensi dell'art. 116 TUF (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione siano derivati danni alla società o a terzi.

L'art. 2391, comma primo, c. c. impone agli amministratori delle società per azioni di dare notizia agli altri

amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata. Gli amministratori delegati devono altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale. L'amministratore unico deve darne notizia anche alla prima assemblea utile.

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

Tale ipotesi di reato consiste nella ripartizione 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.

Soggetti attivi del reato sono esclusivamente i liquidatori.

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

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.
Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

Aggiotaggio (art. 2637 c.c.)

Tale ipotesi di reato consiste nella diffusione di notizie false ovvero nel porre 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 richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Anche questo è un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

Estensione delle qualifiche soggettive (art. 2639 c.c.)

Per tutti i reati previsti dal paragrafo B.1, al soggetto formalmente investito della qualifica o titolare della funzione prevista dalla legge civile è equiparato sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Fuori dei casi di applicazione delle norme riguardanti i delitti dei pubblici ufficiali contro la pubblica amministrazione, le disposizioni sanzionatorie relative agli amministratori si applicano anche a coloro che sono legalmente incaricati dall'autorità giudiziaria o dall'autorità pubblica di vigilanza di amministrare la società o i beni dalla stessa posseduti o gestiti per conto di terzi.

B.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree di attività ritenute più specificamente a rischio, ai fini della presente Parte speciale "B" del Modello, e le correlate "attività sensibili", risultano essere le seguenti:

- Gestione degli adempimenti, delle comunicazioni e delle richieste, anche in occasione di verifiche, ispezioni ed accertamenti da parte degli enti pubblici competenti o delle autorità amministrative indipendenti
    - Rapporti con le Autorità Amministrative Indipendenti (es. Autorità Garante della Concorrenza e del mercato) e gestione delle comunicazioni e delle informazioni a esse dirette, anche in occasione di verifiche ispettive.

- Selezione e assunzione del personale
  - Gestione delle attività di selezione, assunzione e gestione del personale con particolare riferimento a titolo esemplificativo alle seguenti attività:
    - ✓ definizione del piano di fabbisogno del personale;
    - ✓ richiesta di assunzione;
    - ✓ screening dei cv;
    - ✓ analisi delle candidature;
    - ✓ formalizzazione del contratto di assunzione.

- Gestione della contabilità generale e formazione del bilancio
  - Gestione della contabilità generale, con particolare riferimento alle attività di:
    - ✓ rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici (es. gestione e registrazione contabile della fatturazione attiva);
    - ✓ verifica dati provenienti dai sistemi informativi alimentanti;
    - ✓ raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico e consolidato

- Gestione degli adempimenti in materia societaria
  - Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul Bilancio d'Esercizio e nelle attività di verifica della gestione aziendale.
  - Custodia e tenuta dei Libri Sociali.
  - Tenuta delle scritture contabili e dei libri contabili.

- Approvvigionamento di beni e servizi
  - Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività:
    - ✓ Gestione dell'albo fornitori;
    - ✓ selezione del fornitore e valutazione dei requisiti qualificanti;
    - ✓ stipula di accordi quadro di fornitura;
    - ✓ emissione degli ordini.

- Progettazione e commercializzazione di software applicativi per elaboratori
  - Gestione dei rapporti con clienti diretti e distributori, con particolare riferimento alle seguenti attività:
    - ✓ gestione dell'anagrafica clienti;
    - ✓ definizione della scontistica da applicare;

- ✓ formalizzazione dell'offerta;
- ✓ evasione dell'ordine;
- ✓ monitoraggio del credito.

- Gestione delle partnership
  - Gestione dei rapporti con società pubbliche e private con le quali si intende stipulare accordi di partnership, con particolare riferimento alle seguenti attività:
    - ✓ individuazione delle opportunità di partnership commerciali/tecnologiche;
    - ✓ definizione degli accordi con i Partner.

- Gestione delle attività infragruppo
  - Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

B.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale prevede l'espresso divieto, a carico dei Destinatari, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-ter del d.lgs. 231/2001);
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei Destinatari di rispettare, oltre ai principi di controllo interno enunciati nella Parte Generale (cfr. 2.10), i seguenti principi di comportamento:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al socio ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
2. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3. assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
4. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza.
5. porre in essere comportamenti tali da integrare la fattispecie di reato di corruzione tra privati ovvero di istigazione alla corruzione tra privati.

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:

con riferimento al precedente punto 1:

- 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 società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;

con riferimento al precedente punto 2:

- restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale;

con riferimento al precedente punto 3:

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio, del Collegio Sindacale o della società di revisione;

con riferimento al precedente punto 4:

- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti dell'Autorità di Vigilanza, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalla predetta autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

con riferimento al precedente punto 5:

- effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a dipendenti di altre società private;
- effettuare o promettere, in favore dei clienti, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito.

B.4 Responsabile interno

Per ogni area a rischio, come individuate al punto B.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

B.5 Processi strumentali e Sistema dei controlli

Di seguito sono riportati i processi c.d. strumentali/funzionali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato sopra considerate:

- Formazione del Bilancio e adempimenti societari
- Consulenze e incarichi professionali a terzi
- Acquisto di beni e servizi
- Rimborsi spese, anticipi e spese di rappresentanza
- Flussi monetari e finanziari
- Rapporti con la Pubblica Amministrazione
- Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità
- Selezione, assunzione, gestione del personale dipendente

La dettagliata individuazione del sistema dei controlli interni adottato dalla Società per la prevenzione dei Reati in questione (comprensivo, tra l'altro, di regole di comportamento, policy e procedure aziendali, strumenti di tracciabilità e di organizzazione) è contenuta nella documentazione di Risk Assessment redatta preliminarmente all'adozione del Modello Organizzativo. Peraltro, anche successivamente all'esecuzione del Risk Assessment, la Società ha provveduto ad integrare ed ampliare il proprio sistema di controllo per la prevenzione dei Reati societari, attraverso l'implementazione di una serie di azioni di miglioramento dirette a garantire l'effettiva idoneità ed il costante aggiornamento nel tempo del Modello Organizzativo.

I protocolli per la prevenzione dei Reati societari sono costituiti, pertanto, dall'insieme di tali strumenti, nonché dai principi di comportamento e dalle prescrizioni di cui alla presente Parte Speciale. In particolare, a titolo esemplificativo e non esaustivo, la Società è dotata dei seguenti strumenti specifici di controllo e prevenzione in relazione alle Aree a Rischio sopra considerate:

- Formazione del Bilancio di esercizio, consolidato e delle situazioni contabili infrannuali, gestione degli adempimenti societari, gestione dei rapporti con gli Organi sociali e di controllo
- Procedura di gestione della tesoreria e dei flussi monetari e finanziari
- Approvvigionamento beni e servizi (ciclo passivo)

- Manuale di qualificazione dei fornitori
- Gestione omaggi
- Gestione sponsorizzazioni ed erogazioni liberali
- Procedura di gestione del contenzioso
- Procedura di gestione delle risorse umane
- Policy rimborsi spese e trasferte
- Procedura gestione crediti di Gruppo
- Gestione delle informazioni privilegiate e degli obblighi di comunicazione

PARTE SPECIALE "C" - REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI E UTILITÀ DI PROVENIENZA ILLECITA NONCHÉ AUTORICICLAGGIO

C.1 Le tipologie dei reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita (art. 25-octies del Decreto)

Per quanto concerne la presente Parte Speciale "C", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati e indicati all'art. 25-octies del Decreto. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

Ricettazione (art. 648 c.p.)

Il delitto di ricettazione può essere integrato da chiunque – senza che sia configurabile concorso nel reato presupposto – acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto o, comunque, si intromette per farle acquistare, ricevere od occultare, al fine di ottenere per sé o per altri un profitto.

Per la ricorrenza della fattispecie in questione è necessario che il denaro o le cose provengano dalla commissione di un precedente delitto (ad es. furto, rapina, ecc.) che costituisce il presupposto della ricettazione. E', altresì, necessario che l'autore del reato abbia come finalità quella di perseguire – per sé o per terzi – un profitto, che può anche non essere di carattere patrimoniale.

Perché l'autore dei fatti sia punibile per il delitto di ricettazione è necessario che agisca con dolo – anche nella forma eventuale – ossia che sia a conoscenza della provenienza illecita del denaro o delle cose e le voglia acquistare, ricevere, occultare o, dolosamente, voglia intromettersi nel favorire queste condotte.

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

Il delitto di riciclaggio punisce chiunque, senza che sia configurabile concorso nel reato presupposto, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare la identificazione della loro provenienza delittuosa.

Come per il delitto di ricettazione, anche per le ipotesi di riciclaggio, è necessario che il denaro, i beni o le altre utilità (rientrano nella previsione della norma anche le aziende, i titoli, i diritti di credito) provengano dalla commissione di un precedente delitto non colposo (ad es. reati tributari, reati contro il patrimonio, ecc.) che ne costituisce il presupposto.

Perché l'autore dei fatti sia punibile per il delitto di riciclaggio è necessario che agisca con dolo – anche nella forma eventuale – ossia che sia a conoscenza della provenienza illecita del denaro o delle cose e le voglia acquistare, ricevere, occultare o, dolosamente, voglia intromettersi nel favorire queste condotte.

Il fatto è aggravato se commesso nell'esercizio di un'attività professionale.

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

Salvo che la condotta sia riconducibile alle ipotesi di cui all'art. 648 (ricettazione) o all'art. 648-bis (riciclaggio), è punibile chiunque impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, sempre che l'autore non abbia concorso alla realizzazione del reato presupposto (ad es. furto, reati tributari, reati di falso, ecc.).

Sotto il profilo dell'elemento soggettivo, è richiesta la ricorrenza del dolo generico, inteso quale consapevolezza della provenienza delittuosa del bene e volontà della realizzazione della condotta tipica sopra descritta.

Anche in questa fattispecie, è prevista la circostanza aggravante dell'esercizio di un'attività professionale ed è esteso ai soggetti l'ultimo comma dell'art. 648, ma la pena è diminuita se il fatto è di particolare tenuità.

Il riferimento specifico al termine "impiegare", di accezione più ampia rispetto a "investire" che suppone un impiego finalizzato a particolari obiettivi, esprime il significato di "usare comunque". Il richiamo al concetto di

“attività” per indicare il settore di investimento (economia o finanza) consente viceversa di escludere gli impieghi di denaro od altre utilità che abbiano carattere occasionale o sporadico.

La specificità del reato rispetto a quello di riciclaggio risiede nella finalità di far perdere le tracce della provenienza illecita di denaro, beni o altre utilità, perseguita mediante l’impiego di dette risorse in attività economiche o finanziarie.

Il legislatore ha inteso punire quelle attività mediate che, a differenza del riciclaggio, non sostituiscono immediatamente i beni provenienti da delitto, ma che comunque contribuiscono alla “ripulitura” dei capitali illeciti.

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

La norma, introdotta con la L. 186/2014, punisce il soggetto che, avendo commesso o concorso a commettere il reato presupposto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale predetto reato presupposto, in modo tale da ostacolare in maniera concreta l’accertamento della loro provenienza delittuosa.

La norma prevede una fattispecie attenuata qualora il denaro, i beni o le altre utilità provengono da delitto che prevede una pena inferiore nel massimo a cinque anni.

Le condotte di autoriciclaggio non sono tuttavia punibili quando il denaro, i beni o le altre utilità vengono destinati alla mera utilizzazione o al godimento personale.

Le pene sono invece aumentate se i fatti di autoriciclaggio sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

La pena, inoltre, è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto.

Il dolo richiesto dal reato di autoriciclaggio è quello generico, costituito dalla consapevolezza di avere realizzato o contribuito a realizzare un delitto non colposo e volontà di impiegare, sostituire, trasferire, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto. L'oggetto del dolo include altresì la consapevolezza e volontà di agire in modo da ostacolare concretamente l'identificazione della provenienza delittuosa dei beni.

C.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale “C” del Modello, le aree di attività ritenute più specificamente a rischio e le correlate “attività sensibili”, sono:

- Gestione dei flussi monetari e finanziari
    - Gestioni dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività:
        - ✓ autorizzazione e invio dei pagamenti;
        - ✓ inserimento/modifica delle coordinate bancarie del fornitore.

- Approvvigionamento di beni e servizi
    - Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività:
        - ✓ Gestione dell’albo fornitori;
        - ✓ selezione del fornitore e valutazione dei requisiti qualificanti;

- ✓ stipula di accordi quadro di fornitura;
- ✓ emissione degli ordini.

- Progettazione e commercializzazione di software applicativi per elaboratori
  - Gestione dei rapporti con clienti diretti e distributori, con particolare riferimento alle seguenti attività:
    - ✓ gestione dell'anagrafica clienti;
    - ✓ definizione della scontistica da applicare;
    - ✓ formalizzazione dell'offerta;
    - ✓ evasione dell'ordine;
    - ✓ monitoraggio del credito.

- Gestione delle attività infragruppo
  - Gestione dei contratti di acquisto e/o di vendita infragruppo, investimenti infragruppo, transazioni finanziarie infragruppo.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

C.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, di:

- trasferire a qualsiasi titolo, se non per il tramite di banche o istituti di moneta elettronica o Poste Italiane S.p.A., denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore a quello previsto dalla vigente normativa;
- emettere assegni bancari e postali per importi pari o superiori a quello previsto dalla vigente normativa che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- girare per l'incasso assegni bancari e postali emessi all'ordine del traente a soggetti diversi da banche o Poste Italiane S.p.A.;
- effettuare pagamenti su conti correnti esteri nei confronti di persone fisiche residenti in Italia o di enti aventi sede legale in Italia;

- effettuare pagamenti su conti correnti di banche operanti in paesi ricompresi nelle liste “tax heaven” e in favore di società off-shore.
- utilizzare informazioni su clienti, fornitori, operatori acquisite illecitamente al fine di ottenere benefici di qualunque utilità nelle relazioni commerciali;
- riconoscere, in favore dei fornitori, consulenti e/o collaboratori esterni, compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente nel settore di attività interessato.

C.4 Responsabile interno

Per ogni area a rischio, come individuate al punto C.2, l’Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il “Responsabile Interno”).

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell’ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l’OdV nello svolgimento di ogni attività necessaria ai fini dell’espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all’OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all’OdV.

C.5 Processi strumentali e sistema di controllo

Di seguito è riportato, il processi c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato sopra considerate:

- Flussi monetari e finanziari

La dettagliata individuazione del sistema dei controlli interni adottato dalla Società per la prevenzione dei Reati previsti dalla presente Parte Speciale (comprensivo, tra l’altro, di regole di comportamento, policy e procedure aziendali, strumenti di tracciabilità e di organizzazione) è contenuta nella documentazione di Risk Assessment redatta preliminarmente all’adozione del Modello Organizzativo. Anche successivamente all’esecuzione del Risk Assessment, la Società ha provveduto ad integrare ed ampliare il proprio sistema di controllo per la prevenzione dei Reati societari, attraverso l’implementazione di una serie di azioni di miglioramento dirette a garantire l’effettiva idoneità ed il costante aggiornamento nel tempo del Modello Organizzativo.

I protocolli per la prevenzione dei Reati sopra considerati sono costituiti, pertanto, dall’insieme di tali strumenti, nonché dai principi di comportamento e dalle prescrizioni di cui alla presente Parte Speciale. In particolare, a titolo esemplificativo e non esaustivo, la Società è dotata dei seguenti strumenti specifici di controllo e prevenzione in relazione alle Aree a Rischio sopra considerate:

- Formazione del Bilancio di esercizio, consolidato e delle situazioni contabili infrannuali, gestione degli adempimenti societari, gestione dei rapporti con gli Organi sociali e di controllo
- Procedura di gestione della tesoreria e dei flussi monetari e finanziari

- Approvvigionamento beni e servizi (ciclo passivo)
- Manuale di qualificazione dei fornitori
- Gestione omaggi
- Gestione sponsorizzazioni ed erogazioni liberali
- Procedura di gestione delle risorse umane
- Policy rimborsi spese e trasferte
- Procedura gestione crediti di Gruppo

PARTE SPECIALE "D" - REATI DI CRIMINALITÀ INFORMATICA

D.1 Le tipologie dei reati di criminalità informatica (art. 24-bis del decreto)

Per quanto concerne la presente Parte Speciale "D", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24-bis del Decreto, e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Documenti informatici (art. 491-bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici. Per effetto dell'art. 2, co. 1, lett. e) D.Lgs. 7/2016, che ha abrogato l'art. 485 c.p. ("Falsità in scrittura privata") e che ha introdotto una nuova ipotesi di illecito civile, è stato eliminato il riferimento precedentemente contenuto nella norma al "documento informatico privato", con la conseguenza che oggi non hanno più rilievo penale condotte di falsità che ricadono su documenti (anche) informatici privati.

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

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Chiunque, al fine di procurare a sé o 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 ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora cancella, altera o sopprime informazioni, dati o programmi informatici altrui, è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al n. 1) del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

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 è punito con la reclusione da 1 a 5 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

Se il fatto di cui all'art. 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da 1 a 4 anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a 3 anni e con la multa da 51 a 1.032 euro.

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2. da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3. da chi esercita anche abusivamente la professione di investigatore privato.

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.)

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

D.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "D" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, account e profili)
- Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni
- Gestione della progettazione e della installazione dei software applicativi aziendali con particolare riferimento ai rapporti con clienti diretti e distributori
- Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT"
- Gestione e manutenzione dell'hardware e del software e tenuta dell'inventario
- Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici"
- Gestione dei servizi e dei software di firma digitale per l'invio di documenti alla PA

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

D.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale ed ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari di specifici obblighi, strumentali ad un'adeguata esecuzione delle attività di controllo interno previste nella presente Parte Speciale, i seguenti soggetti esterni (di seguito i "Soggetti Esterni"):

- i collaboratori, gli agenti e i rappresentanti, i consulenti e in generale i soggetti che svolgono attività di lavoro autonomo nella misura in cui essi operino nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società;
- i fornitori e i partner (anche sottoforma di associazione temporanea di imprese, nonché di joint-venture) che operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività cosiddette sensibili per conto o nell'interesse della Società.

Tra i Soggetti Esterni così definiti debbono ricondursi anche coloro che, sebbene abbiano il rapporto contrattuale con altra Società del Gruppo, nella sostanza operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale (i) prevede che l'utilizzo delle risorse informatiche e di rete avvenga in modo corretto, in conformità a quanto previsto dalle procedure aziendali interne e nel rispetto delle misure di sicurezza adottate dalla Società; (ii) prevede l'espresso divieto a carico di tutti i Destinatari, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- violare i principi e le procedure aziendali previste nella presente parte speciale;
- accedere in maniera non autorizzata ai sistemi informativi utilizzati da soggetti privati o dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare informazioni a vantaggio dell'azienda o di terzi, o comunque al fine di procurare un indebito vantaggio all'azienda od a terzi;
- formare falsamente (sia sotto il profilo materiale sia per quanto attiene al contenuto) documenti societari aventi rilevanza esterna;
- distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda.
- distruggere, danneggiare, rendere in tutto o in parte inservibile sistemi informatici o telematici altrui o della Società ovvero ostacolarne gravemente il funzionamento;
- intercettare fraudolentemente, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
- rivelare, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle comunicazioni fraudolentemente intercettate relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio virus, worm, troian, spyware, dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- procurarsi, riprodurre, diffondere comunicare o consegnare codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o, comunque, fornire indicazioni o istruzioni idonee al predetto scopo;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o comunque mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti;

I destinatari del Modello interessati dalle aree a rischio sopra individuate e che, per comodità si riportano di seguito, devono agire nel pieno rispetto delle attività di controllo definite dei seguenti protocolli specifici:

- **Gestione delle attività di accesso ai sistemi informatici/telematici e alle applicazioni (autenticazione, account e profili)**
    - La Società deve definire, aggiornare e approvare formalmente le policies aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e all'accesso remoto da parte di terzi soggetti.
    - La Società deve gestire il processo di nomina di amministratore/i di sistema e amministratore/i di database con atto formale, definizione di compiti e attribuzioni ed espressa assunzione della relativa responsabilità nel rispetto di quanto previsto dal Provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008.
    - La Società deve far rispettare il sistema di gestione delle utenze, con particolare riferimento alla definizione di nuove utenze e della loro cancellazione.
    - È vietato per tutti i dipendenti di: (i) introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema I1informatico o telematico protetto da misure di sicurezza; (ii) procurarsi, riprodurre, diffondere, comunicare, I3consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo.
- **Gestione dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni**
    - La Società deve definire, aggiornare e approvare formalmente le policies aziendali, le procedure in materia di sicurezza informatica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai profili di autorizzazione dei singoli utenti.
- **Gestione della progettazione e della installazione dei software applicativi aziendali con particolare riferimento ai rapporti con clienti diretti e distributori**
    - La Società deve definire, aggiornare e approvare formalmente le policies aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e all'accesso remoto da parte di terzi soggetti.
    - La Società deve procedere all'integrazione e alla centralizzazione della gestione informatica per quanto attiene le aree di sviluppo. Per quanto alcune attività possano essere svolte operativamente in periferia, è infatti opportuno che la gestione dell'intero sistema informativo sia uniforme e coordinato.
    - La società deve definire una chiara politica di controllo degli accessi negli ambienti di sviluppo e deve costantemente verificarne l'applicazione.
- **Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT**
    - La Società deve regolamentare in modo chiaro e formalizzato l'accesso fisico ai locali in cui risiedono le infrastrutture IT (attribuzione di facoltà di accesso, misure di sicurezza e di vigilanza e assunzione della relativa responsabilità).
- **Gestione e manutenzione dell'hardware e del software e tenuta dell'inventario**

- La Società deve adottare una procedura che gestisca l'inventario degli asset a supporto delle attività di gestione, che permetta di mantenere la visibilità dello stato delle risorse e ne faciliti la manutenzione, l'implementazione e la gestione e manutenzione di reti.
- La Società deve promuovere controlli finalizzati a garantire la gestione e la manutenzione hardware e software (ivi compresi l'inventario e i divieti o limitazioni di utilizzo) e deve attivare procedure di controllo di installazione di software potenzialmente pericolosi sui sistemi operativi.

- **Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici"**
  - La Società deve definire, aggiornare e approvare formalmente le policies aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento al piano di back up, disaster recovery e alla gestione della posta elettronica.
  - La Società deve promuovere l'utilizzo di sistemi crittografici nella creazione, emissione, archiviazione, conservazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici.
  - La Società deve promuovere momenti di allineamento fra esigenze di business e sistema informativo, ad esempio all'interno di un comitato di indirizzo periodico in cui siano esplicitate le esigenze strategiche e di allineamento con le relative priorità, siano monitorate le attività di adeguamento, e siano assicurate le risorse necessarie.
- **Gestione dei servizi e dei software di firma digitale per l'invio di documenti alla PA**
  - La Società deve definire, aggiornare e approvare formalmente le policies aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento alle misure di protezione dell'integrità e disponibilità delle informazioni messe a disposizione su un sistema accessibile al pubblico, al fine di prevenire modifiche non autorizzate;
  - La Società deve dotarsi di un sistema di risk management sotto il profilo IT che preveda un piano di audit periodico in cui vengono verificati i requisiti di sicurezza che si devono richiamare ai principi previsti dagli Standard ISO 27001.

D.4 Responsabile interno

Per ogni area a rischio, come individuate al punto D.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello;

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

D.5 Processi strumentali e Sistema dei controlli

Di seguito è riportato il processo c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato sopra considerate:

- Gestione dei sistemi informativi

La dettagliata individuazione del sistema dei controlli interni adottato dalla Società per la prevenzione dei Reati previsti dalla presente Parte Speciale (comprensivo, tra l'altro, di regole di comportamento, policy e procedure aziendali, strumenti di tracciabilità e di organizzazione) è contenuta nella documentazione di Risk Assessment redatta preliminarmente all'adozione del Modello Organizzativo. Peraltro, anche successivamente all'esecuzione del Risk Assessment, la Società ha provveduto ad integrare ed ampliare il proprio sistema di controllo per la prevenzione dei Reati in questione, attraverso l'implementazione di una serie di azioni di miglioramento dirette a garantire l'effettiva idoneità ed il costante aggiornamento nel tempo del Modello Organizzativo.

I protocolli per la prevenzione dei Reati societari sono costituiti, pertanto, dall'insieme di tali strumenti, nonché dai principi di comportamento e dalle prescrizioni di cui alla presente Parte Speciale. In particolare, a titolo esemplificativo e non esaustivo, la Società è dotata dei seguenti strumenti specifici di controllo e prevenzione in relazione alle Aree a Rischio sopra considerate:

- Policy sull'utilizzo delle risorse informatiche aziendali
- Procedura gestione utenti

PARTE SPECIALE "E" - INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

E.1 Le tipologie di reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" (art. 25-decies del decreto)

Per quanto concerne la presente Parte Speciale "E", si provvede qui di seguito a fornire l'elenco dei reati in essa contemplati, indicati nell'art. 25-decies del Decreto. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

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

L'art. 377-bis c.p. punisce il fatto di chi induce (mediante violenza o minaccia o con l'offerta o la promessa di danaro o altra utilità) a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere dichiarazioni utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere.

La condotta di induzione a non rendere dichiarazioni (cioè di avvalersi della facoltà di non rispondere ovvero di rendere dichiarazioni false) deve essere realizzata in modo tipico (o mediante violenza o minaccia, ovvero con l'offerta di danaro o di qualunque altra utilità).

Il soggetto passivo è necessariamente un soggetto al quale la legge attribuisca la facoltà di non rispondere: l'indagato (o l'imputato) di reato connesso o collegato (sempre che gli stessi non abbiano già assunto l'ufficio di testimone), nonché a quella ristretta categoria di testimoni (i prossimi congiunti), cui l'art. 199 c.p.p. conferisce la facoltà di astenersi dal testimoniare.

Non è facile immaginare una casistica che possa determinare la responsabilità dell'ente, ma è ipotizzabile il caso di un dipendente imputato o indagato che venga indotto a rendere false dichiarazioni (o ad astenersi dal renderle) per evitare un maggior coinvolgimento della responsabilità risarcitoria dell'ente stesso collegata al procedimento penale nel quale il dipendente è coinvolto.

E.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "E" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Gestione dei contenziosi (es.: civili, tributari, giuslavoristici, amministrativi, penali), in tutti i gradi di giudizio
    - Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

E.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari di:

- offrire denaro, altra utilità o anche soltanto esercitare pressione e/o qualunque forma di condizionamento a coloro che dovessero risultare indagati/imputati (o persone informate sui fatti/testimone, test) in un procedimento penale connesso alla Società al fine di influenzarne il giudizio e/o limitarne la libertà di esprimere le proprie rappresentazioni dei fatti o di esercitare la facoltà di non rispondere accordata dalla legge, al fine di favorire gli interessi della Società o trarne un vantaggio per la medesima;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di cui alla presente Parte Speciale;
- effettuare prestazioni in favore dei consulenti, dei Partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
- violare i principi di controllo previsti nella presente Parte Speciale;
- prendere contatti con dipendenti coinvolti in procedimenti penali, allo scopo di indurli a rendere dichiarazioni atte ad evitare l'eventuale rischio di un coinvolgimento della società.

Inoltre, la Società dovrebbe selezionare i soggetti autorizzati ad interloquire con i dipendenti coinvolti in procedimenti penali, e gli eventuali colloqui intercorsi verbalizzati.

E.4 Responsabile interno

Per ogni area a rischio, come individuate al punto E.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

E.5 Processi strumentali e sistema di controllo

Di seguito sono riportati i processi c.d. strumentali/funzionali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Consulenze e incarichi professionali
- Acquisto di beni e servizi
- Rimborsi spese, anticipi e spese di rappresentanza
- Flussi monetari e finanziari
- Gestione del contenzioso
- Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità
- Selezione, assunzione, gestione del personale dipendente
- Rapporti con la Pubblica Amministrazione
- Produzione e commercializzazione di prodotti

La dettagliata individuazione del sistema dei controlli interni adottato dalla Società per la prevenzione dei Reati previsti dalla presente Parte Speciale (comprensivo, tra l'altro, di regole di comportamento, policy e procedure aziendali, strumenti di tracciabilità e di organizzazione) è contenuta nella documentazione di risk assessment redatta preliminarmente all'adozione del Modello Organizzativo. Peraltro, anche successivamente all'esecuzione del Risk Assessment, la Società ha provveduto ad integrare ed ampliare il proprio sistema di controllo per la prevenzione dei Reati societari, attraverso l'implementazione di una serie di azioni di miglioramento dirette a garantire l'effettiva idoneità ed il costante aggiornamento nel tempo del Modello Organizzativo.

I protocolli per la prevenzione dei Reati in questione sono costituiti, pertanto, dall'insieme di tali strumenti, nonché dai principi di comportamento e dalle prescrizioni di cui alla presente Parte Speciale. In particolare, a titolo esemplificativo e non esaustivo, la Società è dotata dei seguenti strumenti specifici di controllo e prevenzione in relazione alle Aree a Rischio sopra considerate:

- Procedura di gestione dei rapporti con la Pubblica Amministrazione
- Procedura di gestione del contenzioso

.

PARTE SPECIALE "F" - REATI COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

F.1 Le tipologie dei reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies del Decreto)

Per quanto concerne la presente Parte Speciale "F", si provvede qui di seguito a fornire l'elenco dei reati in essa contemplati, indicati nell'art. 25-septies del Decreto. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Omicidio colposo (art. 589 c.p.)

Il reato si configura nel caso in cui si cagioni per colpa la morte di una persona.

Lesioni personali colpose (art. 590 c.p.)

Il reato si configura nel caso in cui si cagionino per colpa ad una persona lesioni gravi o gravissime, a seguito della violazione delle norme per la prevenzione degli infortuni sul lavoro.

Le lesioni si considerano gravi nel caso in cui: a) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; b) il fatto produce l'indebolimento permanente di un senso o di un organo (art. 583, comma 1, c.p.).

Le lesioni si considerano gravissime se dal fatto deriva: a) una malattia certamente o probabilmente insanabile; b) la perdita di un senso; c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; d) la deformazione, ovvero lo sfregio permanente del viso (art. 583, comma 2, c.p.).

Ai fini della integrazione dei suddetti reati, non è richiesto l'elemento soggettivo del dolo, ovvero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza, impudenza o imperizia del soggetto agente, ovvero l'inosservanza da parte di quest'ultimo di leggi, regolamenti, ordini o discipline (art. 43 c.p.).

F.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "F" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Gestione del sistema sicurezza ai sensi del D.Lgs. 81/08 (Testo Unico Sicurezza)
    - Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza sul lavoro ai sensi del D.Lgs. 81/2008 - Testo Unico sulla Sicurezza nei luoghi di lavoro e successive modifiche ed integrazioni.

F.3 Destinatari della Parte speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale:

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, di:

- osservare rigorosamente leggi, regolamenti e procedure in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano l'accesso, il transito e lo volgimento delle attività lavorative presso i locali in uso alla Società;
- fornire adeguati dispositivi di protezione individuale ai proprio dipendenti, conformi alle normative vigenti e in funzione delle mansioni da essi svolte;
- segnalare alle funzioni competenti eventuali inefficienze dei dispositivi di protezione individuali ovvero di altri presidi a tutela della sicurezza nonché, sull'igiene e salute sul lavoro;

E', inoltre vietato:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- violare i principi previsti nella presente parte speciale.

Si precisa che in materia di salute e sicurezza sul lavoro, la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa prevenzionistica vigente, nell'ottica di eliminare, ovvero, laddove ciò non sia possibile, ridurre – e quindi gestire – i rischi lavorativi per i lavoratori; sono stati, inoltre, definiti i compiti e le responsabilità in materia di salute e sicurezza sul lavoro a partire dal Datore di Lavoro fino al singolo Lavoratore.

Per i principi generali di comportamento si rimanda, pertanto, al Documento Generale di Valutazione Rischi predisposto ai sensi del D. Lgs. 81/2008 .

F.4 Responsabile interno

Relativamente a tale tipologia di reati, nell'ottica della previsione di un sistema integrato di controllo, si deve fare riferimento al Datore di Lavoro, al Responsabile del servizio di prevenzione e protezione (RSPP) in quanto qualificabile come controllo tecnico-operativo (o di primo grado), ed all'Organismo di Vigilanza incaricato del controllo sulla efficienza ed efficacia delle procedure rilevanti ai sensi del D. Lgs. n. 231/2001 (o di secondo grado).

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito dell'area a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

F.5 Processi strumentali e sistema di controllo

Di seguito è riportato il processo c.d. strumentali/funzionali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Gestione della Sicurezza sul Lavoro

La dettagliata individuazione del sistema dei controlli interni adottato dalla Società per la prevenzione dei Reati previsti dalla presente Parte Speciale (comprensivo, tra l'altro, di regole di comportamento, policy e procedure aziendali, strumenti di tracciabilità e di organizzazione) è contenuta nella documentazione di Risk Assessment redatta preliminarmente all'adozione del Modello Organizzativo. Peraltro, anche successivamente all'esecuzione del Risk Assessment, la Società ha provveduto ad integrare ed ampliare il proprio sistema di controllo per la prevenzione dei Reati societari, attraverso l'implementazione di una serie di azioni di miglioramento dirette a garantire l'effettiva idoneità ed il costante aggiornamento nel tempo del Modello Organizzativo.

I protocolli per la prevenzione dei Reati in questione sono costituiti, pertanto, dall'insieme di tali strumenti, nonché dai principi di comportamento e dalle prescrizioni di cui alla presente Parte Speciale. In particolare, a titolo esemplificativo e non esaustivo, la Società è dotata del seguente strumento specifico di controllo e prevenzione in relazione alle Aree a Rischio sopra considerate:

- Procedura di gestione della sicurezza

PARTE SPECIALE "G" - REATI DI CRIMINALITÀ ORGANIZZATA

G.1 Le tipologie dei reati di criminalità organizzata (art. 24-ter del Decreto)

Per quanto concerne la presente Parte Speciale "G", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all' art. 24-ter del Decreto e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Associazione per delinquere (Art. 416, ad eccezione del sesto comma, c. p.)

Il reato si configura mediante la condotta di tre o più persone che si associano al fine di commettere delitti. Il fatto vietato consiste anche nella semplice partecipazione ad una associazione per delinquere (cioè ad un gruppo costituito da almeno tre persone che si sono associate allo scopo di commettere delitti): la fattispecie di partecipazione è integrata da un qualunque contributo all'associazione con la consapevolezza del vincolo associativo, non essendo necessario che i reati-fine siano realizzati.

Si consideri che tra le forme di manifestazione del contributo rilevante ai fini della partecipazione è bastevole qualunque figura di aiuto, per esempio la agevolazione nell'ottenimento di un finanziamento.I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, al traffico di organi prelevati da persona vivente, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d.Lgs 286/1998 (art. 416, sesto comma, c.p.)

Il reato si configura mediante la condotta di tre o più persone che si associano al fine di commettere delitti finalizzati alla riduzione o al mantenimento in schiavitù, alla tratta di persone, al traffico di organi prelevati da persona vivente, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 D. Lgs. 286/1998.

Associazione di tipo mafioso anche straniere (Art. 416-bis c. p.)

Il reato si configura mediante la partecipazione ad un'associazione di tipo mafioso formata da tre o più persone. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, di appalti e di 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.

Scambio elettorale politico-mafioso (Art. 416 ter c.p.)

La pena stabilita dal primo comma dell'articolo 416-bis si applica anche a chi ottiene la promessa di voti prevista dal terzo comma del medesimo articolo 416-bis in cambio della erogazione di denaro.

Sequestro di persona a scopo di estorsione (Art. 630 c.p.)

Chiunque sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione, è punito con la reclusione da 25 a 30 anni.

Associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (Art. 74 DPR 309/1990)

Tale ipotesi di reato si configura nel caso in cui tre o più persone si associano allo scopo di coltivare, produrre,

fabbricare, estrarre, raffinare, vendere o mettere in vendita, offrire, cedere, distribuire, commerciare, trasportare, procurare ad altri, inviare, passare o spedire in transito o consegnare per qualunque scopo sostanze stupefacenti o psicotrope. Chi promuove, costituisce, dirige, organizza o finanzia l'organizzazione è punito con la reclusione non inferiore a vent'anni. Chi partecipa è punito con la reclusione non inferiore a dieci anni.

Delitti concernenti la fabbricazione ed il traffico di armi da guerra, esplosivi ed armi clandestine (art. 407 comma 2 lettera a) c.p.p)

Il reato si configura in caso di Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo.

G.2 Aree a rischio

In relazione ai reati di criminalità organizzata e alle condotte criminose sopra esplicitate, tutte le aree indicate al par. 2.9 della parte generale del presente modello sono ritenute a rischio in quanto è sufficiente la partecipazione di tre o più soggetti per la creazione del vincolo associativo di cui all'art. 416 c.p.

G.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari di:

- compiere azioni o tenere comportamenti collusivi che siano finalizzati ad acquisire illecitamente in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di cui alla presente Parte Speciale;
- ricevere o farsi promettere denaro o altra utilità al fine di effettuare scorrette rilevazioni dei prezzi;
- effettuare prestazioni in favore dei consulenti, dei Partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
- omettere informazioni su clienti, fornitori, consulenti giudicate sensibili ai fini del compimento dei reati di cui alla presente parte speciale;
- attivare servizi senza aver preventivamente identificato il cliente secondo le modalità previste dalle procedure interne e richieste dalla legge;

G.4 Responsabile interno

L'applicazione di tali fattispecie di reato è trasversale a tutte le unità organizzative.

G.5 Processi strumentali e sistema di controllo

Ai fini della presente parte speciale "G" del Modello, i processi ritenuti potenzialmente associabili a rischio sono tutti i processi strumentali sopra indicati, in quanto reato trasversale.

Le procedure, policies e, più in generale, i sistemi di controllo adottati dalla Società in relazione ai suddetti processi aziendali (ivi incluso, a titolo esemplificativo, il sistema autorizzativo e di deleghe, gli strumenti di controllo e tracciabilità, etc.), costituiscono parte integrante del presente Modello Organizzativo e si intendono qui integralmente richiamati.

Essendo i reati previsti dalla presente parte speciale trasversali a tutti i processi strumentali individuati, si rimanda all'intero corpus procedurale della Società per una più dettagliata e completa evidenza delle attività di controllo.

PARTE SPECIALE "H" - REATI IN MATERIA AMBIENTALE

H.1 Le tipologie dei reati In Materia Ambientale (art. 25-undecies del decreto)

Per quanto concerne la presente Parte Speciale "H", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati e indicati all'art. 25-undecies del Decreto. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Inquinamento ambientale (art. 452-bis c.p.)

La norma punisce chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:

a. delle acque o dell'aria, o di porzioni estese o significative del suolo o del sotto-suolo;
b. di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Il secondo comma prevede un'ipotesi aggravata, con il conseguente aumento della pena, quando il delitto sia commesso in un'area naturale protetta o sottoposta a specifici vincoli, ovvero in danno di specie animali o vegetali protette.

Il concetto di compromissione o deterioramento "*significativi e misurabili*" riprende la definizione di danno ambientale di cui all'art. 300 del Codice dell'Ambiente di cui al D.Lgs. 152/2006 ("qualsiasi deterioramento significativo e misurabile, diretto o indiretto, di una risorsa naturale o dell'utilità assicurata da quest'ultima") e la stessa nozione comunitaria di "danno ambientale" posta dalla direttiva 2004/35/CE, che usa l'espressione "*mutamento negativo misurabile di una risorsa naturale o un deterioramento misurabile di un servizio di una risorsa naturale, che può prodursi direttamente o indirettamente*".

Disastro Ambientale (art. 452-quater c.p.)

La disposizione prevede che costituiscono disastro ambientale, alternativamente: 1) l'alterazione irreversibile dell'equilibrio di un ecosistema; 2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali; 3) l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Il terzo comma prevede un'aggravante quando il delitto di disastro ambientale sia commesso in un'area naturale protetta o sottoposta a specifici vincoli, ovvero in danno di specie animali o vegetali protette.

Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)

L'art. 452-*quinquies* c.p. introduce le ipotesi in cui l'inquinamento e/o il disastro siano commessi per colpa, prevedendo una riduzione di pena sino ad un massimo di due terzi.

Il secondo comma dell'art. 452-*quinquies* contempla un'ulteriore diminuzione di un terzo della pena per il delitto colposo di pericolo, ovvero quando dai comportamenti di cui agli artt. 452-*bis* e 452-*quater* derivi esclusivamente il pericolo di inquinamento ambientale e disastro ambientale.

Traffico ed abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)

La norma punisce la condotta di chi abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività, prevedendo un aumento di pena se dal fatto deriva il pericolo di compromissione o deterioramento delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo ovvero di un ecosistema, della biodiversità, anche agraria, della flora o della fauna, e un ulteriore aggravamento sanzionatorio se dal fatto deriva pericolo per la vita o per l'incolumità delle persone, la pena è aumentata fino alla metà.

Circostanze aggravanti (art. 452-octies c.p.)

La norma dispone: (i) l'aumento delle pene previste dall'art. 416 c.p. quando l'associazione sia diretta, in via

esclusiva o concorrente, a commettere taluno dei reati ambientali previsti dalla novella; (ii) che sono aumentate le pene previste dall'art. 416-bis c.p. quando l'associazione a carattere mafioso sia finalizzata a commettere taluno dei delitti previsti dal Titolo VI-*bis* del codice penale ovvero all'acquisizione della gestione o comunque del controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi pubblici in materia ambientale; (iii) infine, che entrambe le dette pene siano ulteriormente aumentate se dell'associazione fanno parte pubblici ufficiali o incaricati di un pubblico servizio che esercitano funzioni o svolgono servizi in materia ambientali.

Attività di gestione dei rifiuti non autorizzate (con riferimento all'art. 256, commi 1, 3 e 5, D.Lgs. 152/2006)

Tale reato si configura qualora:

- si effettui una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 del Codice Ambiente;
- si realizzi o gestisca una discarica non autorizzata;
- si effettuino attività non consentite di miscelazione di rifiuti.

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Attività organizzate per il traffico illecito di rifiuti (con riferimento all'art. 260, comma 1 e 2, D.Lgs. 152/2006)

Tale reato si configura qualora al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, si ceda, riceva, trasporti, esporti, importi, o comunque si gestisca abusivamente ingenti quantitativi di rifiuti ed è prevista la pena della reclusione da uno a sei anni.

Se si tratta di rifiuti ad alta radioattività si applica la pena della reclusione da tre a otto anni.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs. 152/2006, art. 258, comma 4, secondo periodo)

Tale reato si configura allorquando, nella predisposizione di un certificato di analisi di rifiuti, si forniscano false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti ovvero si utilizzi un certificato falso durante il trasporto**.**

Falsità ideologica del certificato di analisi dei rifiuti, anche utilizzato nell'ambito del SISTRI – Area Movimentazione, e falsità ideologica e materiale della scheda SISTRI – Area Movimentazione (D.Lgs. 152/2006, art. 260-bis, commi 6, 7, secondo e terzo periodo, e 8 primo periodo- SISTRI)

Tale reato punisce:

- chiunque che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti;
- il trasportatore di rifiuti che omette di accompagnare il trasporto dei rifiuti con la copia cartacea della scheda SISTRI - AREA MOVIMENTAZIONE e, ove necessario sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti; ovvero colui che, durante il trasporto fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati;

Il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI - AREA Movimentazione fraudolentemente alterata.

Scarichi di acque reflue industriali contenenti sostanze pericolose, in assenza di autorizzazione o dopo

che la stessa sia stata sospesa o revocata e scarico nelle acque del mare, da parte di navi o aeromobili, di sostanze o materiali per i quali vige il divieto assoluto di sversamento (con riferimento all'art. 137, commi 2, 3, 5 e 11, D.Lgs. 152/2006)

Tale reato può configurarsi nei seguenti casi:

- scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del D. Lgs. 152/2006;
- scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del D. Lgs. 152/2006, senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente a norma degli articoli 107, comma 1, e 108, comma 4;
- nell'effettuazione di uno scarico di acque reflue industriali, superamento dei valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del D. Lgs. 152/2006, oppure dei limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1;
- mancata osservazione dei divieti di scarico previsti dagli articoli 103 e 104.

Superamento di valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria (D. Lgs. 152/2006, art. 279, comma 5)

Tale reato punisce il superamento dei valori limite di emissione che determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

Omessa bonifica dei siti in conformità al progetto approvato dall'autorità competente (art. 257 commi 1 e 2 D.Lgs. 152/2006)

Tale reato punisce chiunque avendo cagionato l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti.

Cessazione e riduzione dell'impiego di sostanze lesive dell'ozono (L. 549/1993, art. 3, comma 6)

Tale reato si configura qualora non si rispettino le restrizioni/divieti applicate all'impiego di sostanze lesive dell'ozono.

Traffico illecito di rifiuti (D. Lgs. 152/2006, art. 259, comma 1)

Tale reato si configura allorquando si effettui una spedizione di rifiuti costituente traffico illecito ai sensi dell'art.2 del regolamento (CEE) 01/02/1993, n.259 o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'art.1, comma 3, lettere a), b),) e d), del regolamento stesso.

Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.)

Tale reato punisce chiunque distrugge o comunque deteriora in modo significativo un habitat all'interno di un sito protetto. Ai fini dell'applicazione dell'art. 733-bis del codice penale, per 'habitat all'interno di un sito protetto' si intende qualsiasi habitat di specie per le quali una zona sia classificata come zona a tutela speciale a norma dell'art. 4, par. 1 o 2, della Direttiva 79/409/CE, o qualsiasi habitat naturale o un habitat di specie per cui un sito sia designato come zona speciale di conservazione a norma dell'art. 4, par.4, della Direttiva 92/43/CE.

Importazione, esportazione, riesportazione di esemplari appartenenti alle specie protette di cui agli Allegati A, B e C del Regolamento CE n. 338/97 del Consiglio, del 9 dicembre 1996 e ss.mm.ii.; omessa osservanza delle prescrizioni finalizzate all'incolumità degli esemplari appartenenti alle specie protette; uso dei predetti esemplari in modo difforme dalle prescrizioni contenute nei provvedimenti autorizzativi o certificativi; trasporto e transito degli esemplari in assenza del certificato o della licenza prescritti; commercio di piante riprodotte artificialmente in contrasto con le prescrizioni di cui all'art. 7 par. 1 lett. b) Regolamento CE n. 338/97 del Consiglio, del 9 dicembre 1996 e ss.mm.ii.; detenzione, uso per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini

commerciali, offerta in vendita o cessione di esemplari senza la prescritta documentazione (artt. 1 e 2 Legge n. 150/1992)

L'art. 1 della Legge n. 150/1992 punisce:

- chiunque importa, esporta o riesporta, sotto qualsiasi regime doganale, vende, espone per la vendita, detiene per la vendita, offre in vendita, trasporta, anche per conto terzi, o comunque detiene esemplari di specie indicate nell'allegato A, appendice I, e nell'allegato C, parte 1, del regolamento (CEE) n. 3626/82 del Consiglio del 3 dicembre 1982, e successive modificazioni (1 comma);
- chiunque importa oggetti ad uso personale o domestico relativi a specie indicate nel comma 1, senza la presentazione della prevista documentazione CITES emessa dallo Stato estero ove l'oggetto è stato acquistato (2 comma).

L'art. 2, invece, punisce:

- chiunque importa, esporta o riesporta, sotto qualsiasi regime doganale, vende, espone per la vendita, detiene per la vendita, offre in vendita, trasporta, anche per conto terzi, esemplari di specie indicate nell'allegato A, appendici II e III - escluse quelle inserite nell'allegato C, parte 1 - e nell'allegato C, parte 2, del regolamento (CEE) n. 3626/82 del Consiglio del 3 dicembre 1982, e successive modificazioni (1 comma);
- chiunque importa oggetti ad uso personale o domestico relativi a specie indicate nel comma 1, senza la presentazione della documentazione CITES (2 comma).

Falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni previste dall'art. 16, par. 1, lett. a), c), d), e), ed l), del Regolamento CE n. 338/97 del Consiglio, del 9 dicembre 1996 e ss.mm.ii. (art. 3 bis Legge n. 150/1992)

L'art. 3 bis della Legge n. 150/1992 dispone che alle fattispecie previste dall'articolo 16, paragrafo 1, lettere a), c), d), e), ed l), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive modificazioni, in materia di falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni al fine di acquisizione di una licenza o di un certificato, di uso di certificati o licenze falsi o alterati si applicano le pene di cui al libro II, titolo VII, capo III del codice penale.

Detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica (art. 6 Legge n. 150/1992)

Fatto salvo quanto previsto dalla legge 11 febbraio 1992, n. 157, è vietato a chiunque detenere esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica.

Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727--bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta è punito con l'arresto da uno a sei mesi o con l'ammenda fino a 4.000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie. Chiunque, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta è punito con l'ammenda fino a 4.000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie.

Inquinamento doloso di nave battente qualsiasi bandiera (art. 8-9 D.Lgs. n. 202/2007).

Tale reato si configura allorquando il Comandante di una nave, battente qualsiasi bandiera, nonché i membri dell'equipaggio, il proprietario e l'armatore della nave, nel caso in cui la violazione sia avvenuta con il loro concorso, dolosamente o con colpa versano in mare o causano lo sversamento delle sostanze inquinanti di cui all'art. 2, comma 1, lett. b). del D.Lgs. n.202/2007.

H.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "H" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Gestione dei rifiuti
    - Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti.

Eventuali integrazioni delle suddette aree di attività a rischio dovranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

H.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, di:

- compiere azioni o tenere comportamenti che siano o possano essere interpretati come pratiche volte a danneggiare la salute delle persone e/o le componenti naturali dell'ambiente;
- conferire l'attività di gestione dei rifiuti a soggetti non dotati di un'apposita autorizzazione per il loro smaltimento e recupero;
- violare gli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la gestione dei rifiuti;
- utilizzare impianti e apparecchiature in violazione delle disposizioni normative in materia di sostanze ozono lesive.

H.4 Responsabile interno

Per ogni area a rischio, come individuate al punto H.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito dell'area a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di

condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

H.5 Processi strumentali e sistema di controllo

Di seguito è riportato il processo c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Gestione degli adempimenti in materia ambientale

Le procedure, policies e, più in generale, i sistemi di controllo adottati dalla Società in relazione ai suddetti processi aziendali (ivi incluso, a titolo esemplificativo, il sistema autorizzativo e di deleghe, gli strumenti di controllo e tracciabilità, etc.), costituiscono parte integrante del presente Modello Organizzativo e si intendono qui integralmente richiamati.

I destinatari del Modello interessati dalle Aree a Rischio sopra individuate devono agire nel pieno rispetto di quanto previsto dal D.Lgs. 152/2006 "Norme in materia ambientale", nonché dei protocolli specifici previsti dalla seguente procedure aziendale:

- Procedura di gestione ambientale.

PARTE SPECIALE "I" - IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

I.1 Il reato di "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare" (art. 25-duodecies del decreto)

Per quanto concerne la presente Parte Speciale "I", si provvede qui di seguito a fornire una breve descrizione del reato in essa contemplato e indicato all'art. 25-duodecies del Decreto. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità del predetto reato, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

Sulla base delle interviste condotte, in tale ambito è da considerarsi potenzialmente realizzabile la seguente fattispecie di reato.

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Il reato si configura quando il datore di lavoro occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dall' art. 22 del d.lgs. 286/98 ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge il rinnovo, revocato o annullato.

I.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "I" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Selezione e assunzione del personale
    - Gestione delle attività di selezione, assunzione e gestione del personale con particolare riferimento a titolo esemplificativo alle seguenti attività:
        - ✓ definizione del piano di fabbisogno del personale;
        - ✓ richiesta di assunzione;
        - ✓ screening dei cv;
        - ✓ analisi delle candidature;
        - ✓ formalizzazione del contratto di assunzione.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

I.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari di:

- assumere lavoratori stranieri privi di permesso di soggiorno;
- assumere lavoratori il cui permesso sia scaduto – e per il quale non sia richiesto il rinnovo – revocato

o annullato;

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

I.4 Responsabile interno

Per ogni area a rischio, come individuate al punto I.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

I.5 Processi strumentali e sistema di controllo

Di seguito è riportato il processo c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Selezione, assunzione, gestione del personale dipendente.

Le procedure, policies e, più in generale, i sistemi di controllo adottati dalla Società in relazione ai suddetti processi e attività aziendali (ivi incluso, a titolo esemplificativo, il sistema autorizzativo e di deleghe, gli strumenti di controllo e tracciabilità, etc.), costituiscono parte integrante del presente Modello Organizzativo e si intendono qui integralmente richiamati.

I destinatari del Modello interessati dalle Aree a Rischio sopra individuate devono agire nel pieno rispetto delle attività di controllo definite dalla seguente procedura:

- "Gestione delle Risorse Umane"";

PARTE SPECIALE "L" - REATI DI ABUSO DI MERCATO

L.1 Le tipologie dei reati di abuso di mercato (art. 25-sexies del decreto)

Per quanto concerne la presente Parte Speciale "L", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25-sexies del Decreto, e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale

L'art. 9 della legge 18 aprile 2005, n. 62 (Legge Comunitaria per il 2004), che ha recepito la direttiva 2003/6/CE del Parlamento europeo e del Consiglio del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (c.d. abusi di mercato) introduce l'art. 25-sexies nel decreto n. 231/2001. Questa norma estende l'ambito di applicazione della disciplina della responsabilità amministrativa delle persone giuridiche alle condotte che integrano i c.d. abusi di mercato.

Il sistema di sanzioni per i c.d. abusi di mercato definito dal legislatore comunitario è però più complesso in quanto va oltre l'integrazione del decreto n. 231/2001. Infatti, la Legge Comunitaria è intervenuta sia sul codice civile che sul Testo Unico dell'Intermediazione Finanziaria (TUF).

La disciplina della responsabilità dell'ente è stata articolata su due piani: se la fattispecie di illecito presupposto assume rilevanza penale, l'eventuale responsabilità dell'ente sarà accertata in sede giudiziaria (art.25-sexies del Dlgs.231/01)); se invece si tratta di un illecito amministrativo - posto in essere comunque nell'interesse o a vantaggio dell'ente - l'accertamento e l'applicazione delle relative sanzioni spetterà alla Consob (art 187-septies del TUF).

Relativamente alla nozione di informazione privilegiata (informazione price sensitive, ovvero informazione che se resa pubblica potrebbe influire in modo sensibile sui prezzi di strumenti finanziari), l'art. 181 TUF intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.

Relativamente alla nozione di strumenti finanziari, si riportano alcuni strumenti richiamati dall'art. 180 TUF (per l'elenco completo si rimanda art. 1, comma 2 del TUF):

- le azioni o altri titoli rappresentativi di capitale di rischio negoziabili sul mercato dei capitali
- le obbligazioni, i titoli di Stato e gli altri titoli di debito negoziabili sul mercato dei capitali
- i contratti "futures" su strumenti finanziari, su tassi di interesse, su valute, su merci e sui relativi indici, anche quando l'esecuzione avvenga attraverso il pagamento di differenziali in contanti;
- i contratti di scambio a pronti e a termine (swaps) su tassi di interesse su valute, su merci nonché su indici azionari (equity swaps), anche quando l'esecuzione avvenga attraverso il pagamento di differenziali in contanti.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Abuso di informazioni privilegiate (art. 184 TUF)

Tale ipotesi di reato si configura a carico di chiunque, essendo entrato (direttamente) in possesso di informazioni privilegiate in ragione della sua qualità di membro di organo di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dello stesso, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

- acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime – c.d. trading;

- comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio cui è preposto (a prescindere dalla circostanza che i terzi destinatari utilizzino effettivamente l'informazione "comunicata") - c.d. tipping;
- raccomanda od induce altri, sulla base di esse, al compimento di taluna delle operazioni sopra indicate – c.d. tuyautage

I soggetti di cui sopra, in funzione del loro accesso diretto alla fonte dell'informazione privilegiata vengono definiti insider primari. In aggiunta a tali soggetti il nuovo art. 184 TUF estende i divieti di trading, tipping tuyautage a chiunque sia entrato in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose – c.d. criminal insider (es. il pirata informatico che riesce ad entrare in possesso delle informazioni price sensitive).

Manipolazione del mercato (art. 185 TUF)

Tale ipotesi di reato si configura a carico di chiunque diffonda notizie false (c.d. aggiotaggio informativo) o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari (c.d. aggiotaggio operativo). Con riferimento alla diffusione di informazioni false o fuorvianti, si rileva che questo tipo di manipolazione del mercato viene a ricomprendere anche i casi in cui la creazione di un'indicazione fuorviante derivi dall'inosservanza degli obblighi di comunicazione da parte dell'emittente o di altri soggetti obblighi ovvero in ipotesi di omissione.

Di seguito si riportano i reati richiamati dall'art. 187-quinques del TUF:

Illecito amministrativo di abuso di informazioni privilegiate (art. 187-bis TUF):

Tale ipotesi di reato si differenzia rispetto alla corrispondente fattispecie delittuosa in quanto viene richiesto, in capo al soggetto attivo, l'elemento soggettivo del dolo. Inoltre, i divieti di trading, tipping e tuyautage trovano applicazione anche nei confronti di tutti quei soggetti che entrando in possesso di una informazione, conoscevano o potevano conoscere in base all'ordinaria diligenza, il carattere privilegiato delle informazioni stesse (insider secondario).

Infine, si segnala che anche il semplice tentativo può rilevare ai fini dell'applicabilità di tale disciplina in quanto viene equiparato alla consumazione.

Illecito amministrativo di manipolazione di mercato (art. 187-ter TUF):

Tale fattispecie di reato ricomprende, tra le altre:

- le operazioni od 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;
- le operazioni od ordini di compravendita che consentono, tramite l'azione di una o di più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;
- le operazioni od ordini di compravendita che utilizzano artifizi 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.

Per le prime due fattispecie, non può essere assoggettato a sanzione amministrativa chi dimostri di aver agito per motivi legittimi i in conformità alle prassi di mercato ammesse nel mercato interessato.

L.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "L" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Relazioni con il mercato

- Redazione e trasmissione di documenti informativi, prospetti informativi, comunicati, di materiale informativo in qualunque forma predisposti, concernenti la Società e le altre appartenenti al Gruppo, destinate agli investitori, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

L.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale ed ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale, la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-sexies del d.lgs. 231/2001);
- violare i principi previsti nella presente Parte Speciale.

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/01, per tutti i Destinatari, è vietato:

- rivelare a terzi informazioni privilegiate relative alla Società, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate ad utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità;
- concludere operazioni o impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari della Società scendano al di sotto di un certo livello, principalmente per sottrarsi alle conseguenze negative derivanti dal connesso peggioramento del rating degli strumenti finanziari emessi. Questo comportamento deve essere tenuto distinto dalla conclusione di operazioni rientranti nei programmi di acquisto di azioni proprie o nella stabilizzazione degli strumenti finanziari previsti dalla normativa;
- effettuare, anche a mezzo di terzi, operazioni di acquisto, vendita o di altro tipo su strumenti finanziari negoziati in mercati regolamentati, utilizzando le informazioni privilegiate di cui siano venuti a conoscenza nello svolgimento delle proprie attività
- diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo;
- raccomandare o indurre soggetti terzi a compiere le azioni di cui ai punti precedenti punti, sulla base delle medesime informazioni.

Pertanto è fatto obbligo:

- osservare le regole di mercato e le raccomandazioni delle Autorità di settore che presiedono alla formazione del prezzo degli strumenti finanziari, evitando condotte idonee a provocarne una sensibile alterazione, tenuto conto della concreta situazione del mercato interessato;
- osservare le norme di legge e le regole di funzionamento dei mercati volte a garantire la correttezza dell'informazione;

- osservare le prescrizioni previste nella procedura aziendale sulla comunicazione all'esterno di informazioni privilegiate.

L.4 Responsabile interno

Per ogni area a rischio, come individuate al punto L.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina un "Responsabile Interno".

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello;

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

L.5 Processi strumentali e Sistema dei controlli

Di seguito è riportato il processo c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Gestione delle informazioni privilegiate

I destinatari del Modello interessati dalle Aree a Rischio sopra individuate devono agire nel pieno rispetto delle attività di controllo definite dalla seguente procedura:

- Gestione delle informazioni privilegiate e degli obblighi di comunicazione

PARTE SPECIALE "M" - DELITTI IN VIOLAZIONE AL DIRITTO D'AUTORE

M.1 Le tipologie dei delitti in violazione al diritto d'autore (art. 25 novies introdotto dalla l. 99/09)

Per quanto concerne la presente Parte Speciale "M", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25-novies del Decreto, e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Art. 171-bis L. 633/41 (1° comma)

Il primo comma dell'art. 171 è volto a tutelare penalmente il c.d. software, punendo l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore; ma anche l'importazione, la distribuzione, la vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; è altresì punita la predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

La condotta può consistere anzitutto nella abusiva duplicazione, essendo prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro.

Il riferimento all'abusività della riproduzione indica che, sul piano soggettivo, il dolo dell'agente debba ricomprendere anche la conoscenza delle norme extrapenali che regolano la materia.

La seconda parte del comma indica le altre condotte che possono integrare il reato de quo: importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi "piratati". Si tratta di condotte caratterizzate dall'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale.

Infine, nell'ultima parte del comma, il legislatore ha inteso inserire una norma volta ad anticipare la tutela penale del software, punendo condotte aventi ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Sul piano soggettivo, tutte le condotte sono caratterizzate dal dolo specifico di profitto.

Art. 171 L. 633/41 (1° comma, lettera a-bis e 3° comma)

Il delitto di cui all'art. 171 primo comma, lettera a-bis, punisce la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa.

L'inserimento della previsione nel Decreto mira a responsabilizzare tutte quelle aziende che gestiscono server attraverso cui si mettono a disposizione del pubblico opere protette da diritto d'autore.

La norma tutela l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.

Dal punto di vista soggettivo, basta a configurare il reato, il dolo generico, ovvero la coscienza e la volontà di porre in essere la condotta descritta dalla norma.

Il delitto di cui al comma 3 dell'art. 171 è configurabile qualora sia integrata alternativamente una delle condotte menzionate dall'art. 171 (quindi sia l'ipotesi prevista dall'art. 171 lett. a bis, sopra descritta, sia le altre ipotesi indicate dalla norma, ovvero riproduzione, trascrizione, diffusione, messa in vendita, di un 'opera altrui o rivelazione del contenuto, prima che sia reso pubblico; o anche rappresentazione o diffusione di un'opera altrui) ove commesse su un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, o con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti

offesa all'onore od alla reputazione dell'autore.

Il bene giuridico protetto dalla norma di cui al terzo comma consiste nella protezione dei diritti personali del titolare dell'opera, ovvero il suo onore e la sua reputazione, a differenza della ipotesi criminosa precedente che mira a tutelare l'aspettativa di guadagno del titolare dell'opera.

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Art. 171-bis L. 633/41 (2° comma)

Il comma 2 dell'art. 171-bis mira alla protezione delle banche dati; la condotta, invero, si concretizza nella riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; nell'estrazione o reimpiego della banca dati; nella distribuzione, vendita o concessione in locazione di banche di dati.

Per banche dati si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo, con esclusione dei contenuti e dei diritti sugli stessi esistenti.

Art. 171-ter L. 633/41

La norma punisce l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; la riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Perché sia integrato il reato de quo, oltre alla realizzazione di una delle condotte descritte dalla norma, devono ricorrere due requisiti: il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, che costituisce il fine ulteriore che l'agente deve avere di mira perché sia integrato il fatto tipico previsto dalla norma.

Art. 171-septies L. 633/41

La norma punisce i produttori o gli importatori di supporti non soggetti al contrassegno di cui all'art. 181-bis, che non comunicano (ovvero dichiarano falsamente l'assolvimento degli obblighi previsti dall'art. 181-bis) alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti stessi.

Art. 171-octies L. 633/41

La norma punisce chiunque fraudolentemente produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive (cd. decoder) ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

Sono da intendersi ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

M.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "M" del

Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Progettazione e commercializzazione di software applicativi per elaboratori con particolare riferimento: (i) alla gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi; (ii) gestione dei rapporti con clienti diretti e distributori
- .Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE.

Eventuali integrazioni delle suddette aree di attività a rischio dovranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

M.3 Destinatari della parte speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale (cfr. 2.10), la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-novies del d.lgs. 231/2001);
- violare i principi previsti nella presente Parte Speciale.

Inoltre la Società, al fine di evitare il verificarsi dei reati oggetto della presente Parte speciale "H" e considerati, in via potenziale, applicabili alla Società, ha previsto i seguenti principi di controllo che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

- deve essere vietata l'installazione e l'utilizzo non autorizzato di sistemi di file sharing;
- deve essere vietata l'installazione di qualsiasi tipologia di software applicativo non autorizzato ed in assenza di licenza d'uso;
- devono essere predisposti meccanismi di controllo, anche automatico, per il rispetto dei divieti di cui sopra.

I destinatari del Modello interessati dalle aree a rischio sopra individuate e che, per comodità si riportano di seguito, devono agire nel pieno rispetto delle attività di controllo definite dai seguenti protocolli specifici:

- Progettazione e commercializzazione di software applicativi per elaboratori con particolare riferimento alla gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi e alla gestione dei rapporti con clienti diretti e distributori.
  - Al fine di prevenire reati ipotizzabili anche senza l'utilizzo di beni aziendali, si consiglia di:
    - ✓ formulare inviti generali al rispetto delle norme in materia di proprietà intellettuale;

- ✓ elaborare clausole riferite all'osservanza anche da parte dei terzi contraenti delle norme in materia di proprietà intellettuale;
- ✓ vietare l'impiego per finalità aziendali di beni tutelati da diritti acquisiti in elusione dei relativi obblighi o comunque con modalità difformi da quelle previste dal titolare;

o Al fine di prevenire reati ipotizzabili con l'utilizzo di beni aziendali, oltre ai controlli di cui sopra, si consiglia di:

- ✓ vietare l'impiego di beni aziendali al fine di porre in essere condotte che violino la tutela dei diritti d'autore, quale che sia il vantaggio perseguito;
- ✓ controllare i mezzi di comunicazione interni ed esterni alla società (es. sito web, radio ufficiale, stampa, e altri canali ancora), in grado di diffondere opere protette.
- ✓ Infine, nel caso particolare in cui gli illeciti contro la proprietà intellettuale si realizzino con l'impiego di sistemi informatici aziendali, possono rivelarsi utili anche le misure auspicabili anche per la prevenzione dei reati informatici richiamati dagli artt. 24, 24-bis e 25-quinquies del decreto 231, quali ad esempio lo sviluppo, la gestione e il monitoraggio delle infrastrutture informatiche o la presenza del cd. supervisore informatico.
- ✓ Monitorare fenomeni quali: (i) Underlicensing: violazioni delle condizioni di licenza di un software; (ii) Hard disk loading: vendita e relativo acquisto per l'azienda di computer sui quali sono installati; (iii) utilizzazione non autorizzata di banche dati.

- Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE
  - o La Società deve prevedere che l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto;
  - o Tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti;
  - o È fatto espresso divieto di duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);
  - o È fatto espresso divieto di riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.

M.4 Responsabile interno

Per ogni area a rischio, come individuate al punto M.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;

- garantisce, nell'ambito dell'area a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

M.5 Processi strumentali e sistema di controllo

Di seguito è riportato il processo c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Produzione e commercializzazione di prodotti.

Le procedure, policies e, più in generale, i sistemi di controllo adottati dalla Società in relazione ai suddetti processi e attività aziendali (ivi incluso, a titolo esemplificativo, il sistema autorizzativo e di deleghe, gli strumenti di controllo e tracciabilità, etc.), costituiscono parte integrante del presente Modello Organizzativo e si intendono qui integralmente richiamati.

PARTE SPECIALE "N" - REATI CONTRO L'INDUSTRIA E IL COMMERCIO

N.1.le tipologie dei reati contro l'industria e il commercio (art. 25-bis 1 del decreto)

Per quanto concerne la presente Parte speciale "N", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati e indicati all'art. 25-bis/1 del D.lgs.231/2001 e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico dalla Società.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. mappatura) e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriali (art. 517-ter c.p.)

La fattispecie mira a tutelare i diritti di proprietà industriale, acquisiti mediante brevettazione, registrazione o negli altri modi previsti dal D.lgs. 10.02.2005, n. 30 (Codice della proprietà industriale) dando luogo ai cosiddetti titoli di proprietà industriale, la cui usurpazione (o più semplicemente violazione), finalizzata a produrre o impiegare industrialmente i relativi oggetti è fra le condotte penalmente represse dalla previsione in commento

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Turbata libertà dell'industria e del commercio (art. 513 c.p.)

Risponde di tale delitto chiunque adopera violenza (uso di qualsiasi energia fisica su una cosa per effetto della quale la cosa venga danneggiata o trasformata, o ne venga mutata la destinazione) sulle cose, ovvero mezzi fraudolenti (qualsiasi artificio o raggiro capace di trarre in inganno) per impedire o turbare l'esercizio di una industria o di un commercio, se il fatto non costituisce più grave reato.

Tanto la violenza che il mezzo fraudolento devono essere idonei a turbare l'altrui attività commerciale o ad impedirne lo svolgimento.

Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)

Risponde di tale delitto chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza (impiego di energia fisica sulla persona o sulle cose) o minaccia (prospettazione ad una persona di un male ingiusto e futuro, il cui verificarsi dipende dalla volontà del minacciante). Gli atti di concorrenza sono tutti quegli atti compiuti al fine di produrre o vendere di più rispetto agli altri esercenti la stessa attività o attività con essa simile.

Frodi contro le industrie nazionali (art. 514 c.p.)

Il dolo consiste nella volontà di porre in vendita o mettere in circolazione prodotti industriali, con la consapevolezza della contraffazione o alterazione dei nomi, marchi e segni; è altresì necessaria la volontà del nocumento all'industria nazionale.

Frode nell'esercizio del commercio (art. 515 c.p.)

La condotta consiste nel consegnare all'acquirente una cosa mobile non conforme a quella convenuta. Non è necessario che si tratti di un contratto di compravendita, potendo realizzarsi mediante qualunque contratto che comporti la dazione di una cosa mobile da un soggetto ad un altro.

Per 'cosa mobile' è si intende un bene materiale, ad esclusione del denaro, dei diritti su beni immateriali; sono esclusi anche i medicinali, tutelati dall'art. 445 c.p..

La non conformità tra il pattuito e il consegnato può dipendere da diversità di genere o specie, di origine, di provenienza, di qualità, che si riscontra in tutti i casi in cui tra la cosa pattuita e quella consegnata vi è divario di pregio o di utilizzabilità; diversità di quantità, in tutti quei casi in cui sia consegnata una cosa diversa per numero, peso o misura di quella pattuita.

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

Il reato di vendita di prodotti industriali con segni mendaci si consuma nel momento in cui l'opera e il prodotto vengono posti in vendita o messi altrimenti in circolazione e, pertanto, l'elemento oggettivo del delitto deve essere ritenuto sussistente sia allorquando si sia materialmente realizzata la traditio della cosa dal venditore all'acquirente, sia quando vi sia stata una mera attività di porre in vendita, mettendo cioè semplicemente la cosa a disposizione dei potenziali acquirenti. L'elemento oggettivo del reato consiste nella messa in vendita di merce con nomi, marchi o segni distintivi atti a indurre in inganno gli eventuali compratori sulla origine, provenienza o qualità del prodotto.

Nel caso di vendita di prodotti industriali con il marchio contraffatto, trova applicazione l'ipotesi di reato di cui all'art. 474 c.p. e non quella dell'art. 517.

Il reato integra quello di vendita di prodotti industriali con segni mendaci la messa in vendita con la dicitura "made in italy" di un prodotto che non può considerarsi di origine italiana.

Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

La fattispecie delittuosa punisce chiunque pone in vendita o mette altrimenti in commercio come genuine sostanze alimentari non genuine. Questa fattispecie di reato è posta a tutela di un interesse sopraindividuale quale la buona fede negli scambi commerciali la cui violazione si risolve presuntivamente in un pregiudizio per l'ordine economico.

Per "porre in vendita" si intende offrire una determinata sostanza a titolo oneroso.

Per "mettere in circolazione" si intende, invece, qualsiasi forma di messa in contatto della merce con il pubblico, anche a titolo gratuito. Oggetto dell'azione sono le sostanze alimentari non genuine.

La locuzione "sostanze alimentari" è idonea a ricomprendere sia i prodotti provenienti direttamente o indirettamente dalla terra (per coltura o allevamento) sia i prodotti manipolati, lavorati e trasformati e, quindi, provenienti dall'industria, qualsiasi sia il loro stato fisico (solido, liquido o gassoso). La genuinità è la caratteristica fondamentale dei prodotti alimentari e può essere intesa in senso naturale e formale; la genuinità naturale indica la condizione di una sostanza che non abbia subìto processi di alterazione della sua normale composizione biochimica; la concezione formale di genuinità (c.d. genuinità legale) riflette, invece, la conformità della composizione di un prodotto ai requisiti formalizzati in un'apposita normativa. Pertanto, devono considerarsi non genuini sia i prodotti che abbiano subito un'alterazione nella loro essenza e nella loro composizione mediante la commistione di sostanze estranee o la sottrazione di principi nutritivi rispetto a quelli prescritti.

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

La norma incriminatrice punisce chiunque contraffà o comunque altera indicazioni geografiche o denominazioni di origine di prodotti agroalimentari nonché colui che, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i medesimi prodotti con le indicazioni o denominazioni contraffatte.

N.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "N" del Modello, le aree di attività ritenute più specificamente a rischio e le correlate "attività sensibili", sono:

- Progettazione e commercializzazione di software applicativi per elaboratori
    - Gestione delle attività connesse alla progettazione e allo sviluppo di software applicativi.
    - Gestione dei rapporti con clienti diretti e distributori, con particolare riferimento alle seguenti attività:
        - gestione dell'anagrafica clienti;

- definizione della scontistica da applicare;
- formalizzazione dell'offerta;
- evasione dell'ordine;
- monitoraggio del credito.

Eventuali integrazioni delle suddette aree di attività a rischio dovranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

N.3 Destinatari della parte speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale, la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art 25 bis 1 del Decreto);
- fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di cui alla presente Parte speciale;
- violare i principi e le procedure aziendali previste nella presente parte speciale.

E' fatto obbligo ai soggetti, come sopra individuati, di:

- rispettare la legge e le procedure aziendali interne, in tutte le attività finalizzate alla messa in vendita di prodotti;
- osservare le norme di legge poste a tutela del consumatore.

N.4 Responsabile interno

Per ogni area a rischio, come individuate al punto N.2, l'Amministratore delegato della Società, o un dirigente da questi incaricato, nomina uno o più soggetti interni (il "Responsabile Interno").

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito dell'area a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni

di vigilanza e controllo;

- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'OdV.

N.5 Processi strumentali e sistema di controllo

Di seguito è riportato il processo c.d. strumentale/funzionale nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

- Produzione e commercializzazione di prodotti.

Le procedure, policies e, più in generale, i sistemi di controllo adottati dalla Società in relazione ai suddetti processi e attività aziendali (ivi incluso, a titolo esemplificativo, il sistema autorizzativo e di deleghe, gli strumenti di controllo e tracciabilità, etc.), costituiscono parte integrante del presente Modello Organizzativo e si intendono qui integralmente richiamati.

I destinatari del Modello interessati dalle aree a rischio sopra individuate devono agire nel pieno rispetto delle attività di controllo definite dalla seguente procedura:

- Progettazione e sviluppo software