Modello di Organizzazione, Gestione e Controllo

Parte speciale

LDB Medical Care S.r.L.

Sommario

La struttura organizzativa adottata dall'azienda

L'azienda è dotata di un'organizzazione gerarchica e formalizzata che consenta la chiara definizione di attribuzione delle responsabilità, quantifichi i contenuti delle singole posizioni, evidenzi le linee di dipendenza gerarchica, funzionale e di riporto.

La società, definendo compiti e responsabilità ed adottando procedure aziendali ben precise, intende identificare tempestivamente gli interlocutori di riferimento, responsabilizzare il personale dipendente circa la correttezza e trasparenza nelle relazioni con gli interlocutori societari, la tracciabilità e documentabilità dell'operato svolto.

A maggior chiarimento si evidenzia che per la LDB Medical Care S.r.L. il Modello di gestione e controllo ex D.Lgs 231, il Modello Organizzativo - Parte Speciale, la Mappatura ed Analisi dei rischi diretti, la Mappatura ed Analisi dei rischi strumentali, il Documento di Valutazione dei Rischi, il Documento di Valutazione dei Rischi da Interferenze, il Documento della Policy di Privacy Aziendale, sono documenti tra loro integrati e funzionali al raggiungimento delle migliori performance aziendali.

Le informazioni relative ai vari concetti espressi sul presente Modella Organizzativo - Parte Speciale, in aderenza al Modello 231 aziendale, se non presenti, sono comunque riportati e reperibili nei vari documenti sopra elencati.

Articolazione dei poteri e sistema delle deleghe

1. Principi ispiratori del sistema di articolazione dei poteri delle deleghe

Il sistema adottato delle deleghe e dei poteri costituisce parte integrante e sostanziale del Modello 231 aziendale. Il principio cui l'azienda ispira la propria struttura organizzativa e la propria attività è quello in base al quale solo i soggetti muniti di specifici e formali poteri possono assumere, in suo nome e per suo conto, obbligazioni verso terzi. I principi ispiratori di tale sistema sono:

- la tempestiva e costante informazione circa la titolarità dei poteri delegati ed i relativi cambiamenti;
- la verifica periodica del rispetto dei poteri così come delegati;
- le dichiarazioni periodiche in cui sia determinata nel Modello la cadenza con le quali coloro che hanno ricevuto deleghe di poteri confermino il rispetto degli stessi nonché dei principi del codice etico e l'assenza di conflitti di interesse;
- la verifica periodica dell'adeguatezza del sistema delle deleghe.

A tutti i poteri attribuiti mediante delega degli stessi, corrispondono esattamente mansioni e responsabilità come riportate nell'organigramma della società.

Il sistema dei poteri e delle deleghe prevede, se non diversamente previsto dai contratti accettati dalle parti, che:

- ogni destinatario del presente Modello che, per conto dell'azienda intrattiene rapporti negoziali e/o di rappresentanza con l'esterno, deve essere dotato di idonea procura;
- tutti coloro (ivi compreso anche i dipendenti o gli organi sociali) che intrattengono per conto dell'azienda rapporti con la Pubblica Amministrazione, devono essere dotati di delega formale in tal senso;
- ciascuna delega definisce in dettaglio i poteri del delegato e del soggetto.

L'Organismo di Vigilanza verifica periodicamente il sistema delle deleghe e delle procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche.

Il conferimento della procura è seguito da una lettera di accompagnamento da trasmettere al procuratore unitamente all'atto di conferimento della procura e contenente il richiamo al Modello, alle disposizioni del Codice Etico ed alle procedure operative interne.

2. Il sistema dei poteri e delle deleghe

Il principio della segregazione delle responsabilità è applicato in azienda in linea con quanto consentito dalla normativa vigente. I poteri di firma e di rappresentanza sono rilasciati dall'Amministratore Unico e sono revocabili in qualsiasi momento attraverso una semplice notifica a seguito della decisione della società. Il sistema dei poteri e delle deleghe prevede l'attribuzione dei poteri di rappresentanza sia ad altri eventuali amministratori delegati, sia ad ulteriori procuratori (come consulenti esterni, dipendenti, ecc.). I poteri rappresentativi (sia degli amministratori che dei procuratori) sono distinti in formali ed operativi. Mentre i poteri elencati sono indistintamente attribuiti a ciascun amministratore, le deleghe dei procuratori sono conferite in funzione delle attività svolte da ciascuno.

Nell'azienda le procure si dividono in: *(i)* operative, per atti di gestione ordinaria; *(ii)* di rappresentanza; *(iii)* di responsabilità.

Per determinare categorie di atti che prevedano un impegno ultra annuale o che superino uno specifico importo, è prevista l'autorizzazione del CdA o dell'Amministratore Unico, fatti salvi i casi di urgenza specificatamente approvati.

3. Deleghe rilasciate

Le deleghe rilasciate sono parte integrante del Modello aziendale e visionabili nel relativo documento.

Finalità della parte speciale

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nella società, la commissione di reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale ha lo scopo di:

- indicare le attività, procedure, regole di comportamento per evitare di incorrere nei reati evidenziati dal risk assessment;
- sensibilizzare tutti coloro che, in ogni configurazione collaborativa e rapporto di lavoro, hanno relazioni con la LDB Medical Care S.r.L., alla osservanza del Modello, ai fini della corretta applicazione dello stesso;
- fornire all'OdV ed alle altre funzioni aziendali, gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutto il personale dovrà adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuti dei seguenti documenti:

- Modello di Organizzazione, gestione e controllo - Parte Generale;
- Modello di Organizzazione, gestione e controllo - Parte Speciale;
- Codice Etico;
- Sistema disciplinare;

- Statuto Organismo di Vigilanza;
- Sistema di Deleghe e Procure;
- Procedure e Mansionari;
- Ordini di servizio;
- Comunicazioni organizzative;
- Sistemi di gestione delle problematiche di sicurezza e ambientali;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto 231/01.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

Struttura della parte speciale

La presente Parte Speciale individua i reati specifici e le aree di attività a rischio reato, già riportate nel Modello parte generale - Sezioni I, II, III, prese in considerazione dal Decreto 231/01, e considerate sensibili dalla LDB Medical Care S.r.L. a seguito del risk-assessment, le procedure specifiche da adottare per prevenire i reati, le regole di comportamento da seguire, i controlli che possono essere disposti da parte dell'OdV.

REATI - ATTIVITÀ - PROCEDURE - REGOLE DI COMPORTAMENTO

1. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Fattispecie di reato.

Gli artt. 24 e 25 del Decreto 231 richiamano le fattispecie di reato:

- corruzione per l'esercizio della funzione e ambito applicativo (artt. 318 e 320 c.p.);
- corruzione per un atto contrario ai doveri di ufficio, circostanze aggravanti e ambito applicativo (artt. 319, 319-bis e 320 c.p.);
- corruzione in atti giudiziari (art. 319 ter c.p.);
- induzione indebita a dare o promettere utilità (art. 319-quater c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- concussione (art. 317 c.p.);
- truffa in danno dello stato o di altro ente pubblico (art. 640, comma 2, n. 1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);
- frode informatica (art. 640 ter c.p.);
- malversazione a danno dello stato (art. 316 bis c.p.)
- indebita percezione di erogazioni a danno dello stato (art. 316-ter c.p.);
- induzione a non rendere o a rendere dichiarazioni mendaci alla autorità giudiziaria (art. 377-bis c.p.).

1.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere e dalle risposte fornite in sede di intervista, è emerso che le attività a rischio di commissione dei sopra elencati reati sono le seguenti:

- gestione dei rapporti con la P.A.;
- gestione di contenziosi giudiziali e stragiudiziali
- acquisizione e gestione di contributi, sovvenzioni e finanziamenti concessi da soggetti pubblici;
- partecipazioni a bandi di gara indetti dalla P.A.;
- gestione del rapporto contrattuale con gli enti concedenti i servizi;
- predisposizione di bandi di gara o richieste di offerta;
- aggiudicazione dell'appalto.

1.2 - LE PROCEDURE SPECIFICHE

Tutti i Destinatari devono adottare una condotta conforme a quanto qui prescritto al fine di prevenire il verificarsi dei reati.

Rapporti con la P.A.

Tutti coloro che hanno rapporti con soggetti appartenenti alla P.A. o che sono coinvolti in occasione di ispezioni e/o di verifiche da parte della P.A., devono nel primo caso *(i)* osservare l'apposita procedura che disciplina le modalità operative per la gestione dei rapporti con la P.A., compilando una scheda di evidenza; nel secondo caso *(ii)* osservare l'apposita procedura che disciplina le modalità operative per la gestione dei rapporti con la P.A in caso di ispezioni e/o verifiche, compilando una scheda denominata "riepilogo incontri con P.A.".

Acquisizione e gestione di contributi, sovvenzioni e finanziamenti concessi da soggetti pubblici

I responsabili di area devono osservare una procedura che presidia il rischio di presentazione di falsa documentazione per il conseguimento di somme indebite provenienti dalla differenza di costi tra abbonamenti ordinari e abbonamenti speciali (disabili, e anziani a basso reddito).

1.3 - REGOLE DI COMPORTAMENTO

Al fine di evitare il verificarsi dei reati nei confronti della Pubblica Amministrazione e del Patrimonio previsti dal Decreto Legislativo n. 231/01, i destinatari del presente Modello devono:

- attenersi alle seguenti condotte:
  a) osservare rigorosamente tutte le leggi, i regolamenti e le procedure che disciplinano le attività aziendali che comportano contatti e/o rapporti con Enti Pubblici, Pubbliche Amministrazioni e/o Pubblici Ufficiali, Incaricati di Pubblici Servizi e persone esercenti un servizio di pubblica necessità;
  b) improntare i rapporti con Enti Pubblici, Pubbliche Amministrazioni e/o Pubblici Ufficiali, Incaricati di Pubblici Servizi e persone esercenti un servizio di pubblica necessità alla massima trasparenza, correttezza ed imparzialità;
  c) gestire e verificare costantemente, mediante il controllo da parte dei Responsabili sui collaboratori che effettuano attività nei confronti di enti pubblici, che qualsiasi contatto o rapporto, anche occasionale, con i medesimi enti pubblici sia svolto in modo lecito e regolare. I responsabili devono esercitare una supervisione sistematica e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.
- evitare di:
  a) porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/01);
  b) porre in essere, collaborare o dare causa alla realizzazione di comportamenti che violino i principi e le procedure aziendali previste nel presente Modello;
  c) relazionarsi con la Pubblica Amministrazione quando il soggetto sia portatore di interessi personali, diversi da quelli della Società.
- astenersi:
  a) dall'usare la propria posizione al fine di ottenere un beneficio o un privilegio per la Società;
  b) dal richiedere contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, dalla Pubblica Amministrazione, da altri enti pubblici o dalla Comunità Europea o da altri organismi pubblici di diritto internazionale, mediante la presentazione di dichiarazioni non veritiere e/o di documenti falsi e/o mediante l'omissione di informazioni dovute;
  c) dall'usare contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, dalla Pubblica amministrazione, da altri enti pubblici o dalla Comunità Europea o da altri organismi pubblici di diritto internazionale, ottenuti mediante la presentazione di dichiarazioni non veritiere e/o di documenti falsi e/o mediante l'omissione di informazioni dovute;
  d) dal corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di somme ai dipendenti e/o Rappresentanti della Pubblica Amministrazione o di altri Enti Pubblici della Comunità Europea o di altri organismi di diritto internazionale o a loro familiari, a titolo di erogazioni, finanziamenti, contributi per scopi diversi da quelli cui erano originariamente destinati;
  e) dal corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un Pubblico funzionario o a dipendenti e/o Rappresentanti della Pubblica Amministrazione o altri Pubblici Funzionari della Comunità Europea o di altri organismi di diritto internazionale o a loro familiari, allo scopo di:
     - vendere beni e servizi alla Pubblica Amministrazione o prestare alla stessa un servizio;

- ottenere concessioni o licenze dalla Pubblica Amministrazione che, in altro modo, non si sarebbero potute ottenere;
- ottenere trattamenti privilegiati o di favore da parte della Pubblica Amministrazione;
- ottenere trattamenti agevolati da parte delle Autorità di Vigilanza e di controllo (Polizia giudiziaria, ecc.);

f) dal corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un Pubblico funzionario o a dipendenti e/o Rappresentanti della Pubblica Amministrazione o a loro familiari nel caso in cui la Società sia parte di un procedimento giudiziario;

g) dal distribuire e/o ricevere omaggi e/o regali al di fuori delle pratiche aziendali ammesse (ovvero eccedenti le normali pratiche commerciali o di cortesia) comunque rivolti ad ottenere trattamenti di favore nella conduzione di qualsiasi attività aziendale, anche in quei Paesi in cui offrire regali o doni risulti una prassi diffusa in segno di cortesia. Gli omaggi consentiti si caratterizzano per l'esiguità del loro valore (con ciò intendendosi un valore indicativo pari ad un massimo di euro 200,00) e sono volti a promuovere iniziative di carattere benefico o culturale o l'immagine della Società; in ogni caso, gli omaggi devono essere appropriati, non contrastare con la normativa e non devono comunque essere interpretati come richiesta di favori in contropartita. Omaggi di valore superiore devono essere considerati sponsorizzazioni e, come tali, essere trattati secondo le specifiche procedure aziendali;

h) dall'accordare vantaggi di qualsiasi natura (promesse di assunzione, promesse di consulenza, ecc.) a un Pubblico Funzionario o a dipendenti e/o Rappresentanti della Pubblica Amministrazione o ad altri Pubblici Funzionari della Comunità Europea o di altri organismi di diritto internazionale o a loro familiari;

i) dal porre in essere artifici e/o raggiri, tali da indurre in errore ed arrecare un danno allo Stato o ad altro Ente Pubblico o all'Unione Europea o ad organismi di diritto internazionale, per realizzare un ingiusto profitto;

j) dal corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità nei rapporti con Rappresentanti delle Forze Politiche e/o di associazioni portatrici di interesse o loro familiari, per promuovere o favorire interessi della Società, anche a seguito di illecite pressioni;

k) dall'eludere i divieti di cui alle lettere da c) a f) e di cui alla lettera i) ricorrendo a forme diverse di aiuti e/o contribuzioni che, sotto qualsivoglia forma e/o denominazione (ad esempio, sponsorizzazioni, incarichi, consulenza, pubblicità) abbiano, invece, le stesse finalità sopra vietate;

l) dal ricorrere a mezzi di pagamento non previsti dalle procedure aziendali interne e/o da quelle indicate nel Modello, senza la preventiva autorizzazione del Responsabile;

m) dall'accettare da Enti Pubblici o da privati, in proprio o tramite terzi, pagamenti, elargizioni, vacanze gratuite, trasferte, regali o altre utilità del valore indicativo superiore ad € 200,00 che possano condizionarne l'attività.

1.4 - I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale del Modello, l'OdV effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui agli artt. 24 e 25 del Decreto, commessi nell'interesse o a vantaggio della Società, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Come già riportato nella Parte Generale, l'Amministratore Unico ha avocato a sé l'incarico di OdV il quale risulta così il principale referente per le fattispecie di reato individuati in questa sezione.

2. REATI SOCIETARI

Fattispecie di reato:

L'art. 25-ter del Decreto 231 richiama le fattispecie di reato:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);
- omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- impedito controllo (art. 2625 c.c.);
- corruzione tra privati (art. 2635 c.c.)
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggiotaggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

2.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere è emerso che le attività a rischio di commissione dei suddetti reati sono le seguenti:

- predisposizione delle comunicazioni ai soci relative alla situazione economica, patrimoniale e finanziaria della società;
- gestione dei rapporti con i soci e con il collegio sindacale;
- operazioni relative al capitale sociale (gestione dei conferimenti, degli utili, delle riserve ed operazioni sul capitale in genere).

2.2 - LE PROCEDURE SPECIFICHE

In vista della redazione del bilancio annuale, tutte le funzioni coinvolte nella attività di formazione dello stesso devono fornire i dati e le notizie richiesti dal responsabile amministrativo della Società, il quale è tenuto a compilare e a controfirmare per accettazione una check-list che permetta di valutare con ragionevole certezza la completezza dei dati contabili.

2.3 - REGOLE DI COMPORTAMENTO

Al fine di evitare il verificarsi dei reati societari previsti dal D.Lgs. 231/01, i Destinatari del presente Modello devono:

- attenersi alle seguenti condotte:
  a) agire, ciascuno secondo la propria funzione, la propria mansione o il proprio incarico, in osservanza dei principi di correttezza, trasparenza e collaborazione;
  b) nello svolgimento delle procedure volte alla formazione del bilancio, delle situazioni contabili periodiche e delle comunicazioni sociali in generale, mantenere un comportamento improntato ai principi di correttezza, trasparenza e collaborazione, assicurando il rispetto delle norme di legge, dei regolamenti e delle procedure aziendali;
  c) nell'acquisizione, elaborazione e comunicazione delle informazioni destinate a consentire ai Soci di formarsi opinioni e/o giudizi sulla situazione patrimoniale, economica e finanziaria della Società, mantenere un comportamento improntato ai principi di correttezza, trasparenza e collaborazione, assicurando il rispetto delle norme di legge, dei regolamenti e delle procedure aziendali;

d) fornire informazioni veritiere ed appropriate sulla situazione economica, patrimoniale e finanziaria della Società;
e) assicurare il regolare funzionamento della Società e degli Organi sociali, agevolando e garantendo ogni forma di controllo interno nonché promuovendo la libera e corretta formazione ed assunzione delle decisioni assembleari;
f) osservare scrupolosamente tutte le norme di legge poste a tutela dell'integrità ed effettività del capitale sociale, nonché le procedure aziendali fondate su tali norme;
g) rispettare, in caso di riduzione del capitale sociale, di fusione e/o di scissione, le norme di legge poste a tutela dei creditori;
h) osservare le leggi in materia di tutela della concorrenza e del mercato e vigilare sulla perfetta osservanza delle stesse;
i) effettuare con tempestività, correttezza, completezza e buona fede tutte le comunicazioni previste dalla legge;
j) improntare i rapporti con i mass media al rispetto del diritto all'informazione, secondo criteri di accuratezza, coerenza con i principi e le politiche della Società ed in conformità con le leggi, le regole e le pratiche di condotta professionale;

- evitare di:
  a) porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-ter del D.Lgs. 231/01);
  b) porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, seppur non costituiscano di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano diventarlo;
  c) porre in essere, collaborare o dare causa alla realizzazione di comportamenti che violino i principi e le procedure aziendali previste nel presente Modello;
- astenersi:
  a) dall'abusare delle proprie funzioni e poteri statutariamente previsti;
  b) dal predisporre e/o comunicare dati falsi, lacunosi o in ogni modo scorretti al fine di fornire una descrizione non veritiera della situazione patrimoniale, economica e finanziaria della Società;
  c) dall'alterare e/o comunicare dati falsi, lacunosi o in ogni modo scorretti in relazione alla stesura di eventuali prospetti informativi al fine di fornire una descrizione non veritiera della situazione patrimoniale, economica e finanziaria della Società;
  d) dall'omettere dati ed informazioni al fine di fornire una descrizione non veritiera della situazione patrimoniale, economica e finanziaria della Società;
  e) dal restituire i conferimenti e/o esentare i soci dall'effettuarli, al di fuori dei casi specificatamente previsti dalla legge;
  f) dal ripartire utili o acconti su utili non effettivamente conseguiti o destinati a costituire riserva;
  g) dal ripartire riserve, anche non costituite con utili, che per legge non possono essere distribuite;
  h) dal formare e/o aumentare il capitale sociale in modo fittizio;
  i) dall'effettuare operazioni di riduzione del capitale sociale, fusioni o scissioni in violazione delle disposizione di legge a tutela dei creditori e dei terzi in genere;
  j) in fase di liquidazione, dal ripartire fra i soci i beni della Società prima del pagamento dei creditori sociali;
  k) dal mantenere condotte, attive e/o omissive, che impediscano od ostacolano l'esercizio regolare delle attività di controllo interno o di revisione sociale;

l) dal porre in essere atti simulati e/o fraudolenti, nonché diffondere notizie non veritiere al fine di alterare la regolare formazione della volontà assembleare;
m) dal porre in essere atti simulati e/o fraudolenti, nonché diffondere notizie non veritiere che possano, direttamente o indirettamente, alterare sensibilmente il prezzo di strumenti finanziari;
n) dall'esporre nella documentazione e nelle comunicazioni fatti non rispondenti al vero o occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società;
o) dall'omettere di effettuare, con dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalla legge e dalla normativa applicabile, nonché la trasmissione di dati e documenti previsti dalla normativa o specificamente richiesti dalle Autorità Pubbliche di Vigilanza
p) dall'ostacolare il regolare esercizio delle funzioni proprie delle Autorità Pubbliche di Vigilanza, anche e soprattutto in sede di ispezione (a titolo esemplificativo, ma non esaustivo, rifiuti pretestuosi, espressa opposizione, comportamenti ostruzionistici);
q) dall'utilizzare fondi, percepiti a qualsivoglia titolo o finalità, per scopi diversi da quelli per i quali il finanziamento è stato erogato;
r) dall'utilizzare mezzi di pagamento non previsti dalle procedure interne aziendali e/o dalla prassi di mercato, salvo previa autorizzazione e presentazione di adeguata documentazione;
s) dal divulgare ai mass media informazioni false o, comunque, non rispondenti al vero.

2.4 - I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale del Modello, relativamente ai suoi poteri e doveri ivi compreso quello, discrezionale, di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Società. L'Organismo di Vigilanza dovrà esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni. Inoltre, i compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

(i) proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
(ii) monitorare il rispetto delle procedure interne per la prevenzione dei reati societari. L'OdV è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;
(iii) esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute. A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

3. REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

Fattispecie di reato.

L'art. 25-septies del Decreto 231 richiama le fattispecie di reato:

- omicidio colposo (art. 589 c.p.)
- lesioni personali colpose gravi o gravissime (art. 590 comma 3 c.p.)

3.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere e dalle risposte fornite in sede di intervista, è emerso:

- per quanto al reato di omicidio colposo: Non è possibile escludere dall'inventariazione delle aree/attività aziendali, alcun ambito di attività, poiché tali reati possono astrattamente interessare la totalità delle componenti aziendali. L'analisi delle possibili modalità attuative coincide con la valutazione dei rischi lavorativi effettuata dall'azienda sulla scorta della legislazione prevenzionistica vigente, ed in particolare dagli artt. 28 e ss. T.U.
- per quanto al reato di lesioni personali colpose gravi o gravissime, le attività a rischio di commissione dei reati, sono quelle riferibili a:
  - non rispetto della normativa in materia di sicurezza sul luogo di lavoro;
  - mancata individuazione dei rischi aziendali esistenti e loro recepimento nel DVR;
  - omessa gestione del sistema di prevenzione e protezione della salute e della sicurezza dei lavoratori (con particolare riferimento alla predisposizione delle procedure rilevanti e al monitoraggio circa la loro corretta applicazione);
  - mancata formazione ed informazione dei lavoratori, con particolare riguardo alle mansioni agli stessi assegnate e alle qualifiche richieste per lo svolgimento di ciascuna attività;
  - mancato monitoraggio, messa in sicurezza e manutenzione dei luoghi di lavoro con personale della Società o con presenza contemporanea di manodopera esterna di più enti appaltatori;
  - mancata gestione e monitoraggio degli appalti in generale;
  - mancanza del sistema delle deleghe e procure in materia di sicurezza.

Eventuali modifiche o integrazioni delle suddette attività a rischio reato sono rimesse alla competenza dell'organo amministrativo secondo quanto indicato nella Parte Generale del Modello.

3.2 - LE PROCEDURE SPECIFICHE

La LDB Medical Care S.r.L. ha dato mandato alla società Tecno Tomassetti S.r.L. di redigere le procedure specifiche e le istruzioni operative per la esecuzione in sicurezza delle varie attività lavorative aziendali e dell'utilizzo di mezzi, attrezzature e sostanze, nonché sui rischi presenti per mansione e sulle specifiche misure di prevenzione e protezione da adottare, nonché di predisporre il Documento di Valutazione dei Rischi e il Documento di Valutazione dei Rischi Interferenti, ai sensi del D.lgs. 81/08.

3.3 - REGOLE DI COMPORTAMENTO

Principi di comportamento

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori così come individuati dall'art. 15 Decreto Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del medesimo decreto si prevede quanto segue:

La politica aziendale in tema di sicurezza

La politica per la sicurezza e salute sul lavoro adottata dalla Società deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i lavoratori. Tale politica assume come essenziali:

- una chiara affermazione della responsabilità dell'intera organizzazione aziendale, dal Datore di Lavoro al singolo Lavoratore, nella gestione delle tematiche relative alla salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze;
- l'impegno a considerare tali tematiche come parte integrante della gestione aziendale;
- l'impegno al miglioramento continuo ed alla prevenzione;
- l'impegno a fornire le risorse umane e strumentali necessarie;
- l'impegno a garantire che i Destinatari, nei limiti delle rispettive attribuzioni, siano sensibilizzati a svolgere la propria attività nel rispetto delle norme sulla tutela della salute e sicurezza;
- l'impegno al coinvolgimento ed alla consultazione dei Lavoratori, anche attraverso il RLS;
- l'impegno ad un riesame periodico della politica per la salute e sicurezza adottato al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società.

Il processo di pianificazione

La Società, con cadenza periodica:

- definisce gli obiettivi finalizzati al mantenimento e/o miglioramento delle misure di prevenzione e protezione;
- predispone un piano per il raggiungimento di ciascun obiettivo, individua le figure/strutture coinvolte nella realizzazione del suddetto piano e attribuisce dei relativi compiti e responsabilità; definisce le risorse, anche economiche, necessarie;
- prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

L'organizzazione del sistema

Per quanto alla organizzazione aziendale contro i reati di cui si tratta, si rimanda alla Sezione III Paragrafo 3 del Modello.

Informazione e formazione

A - Informazione

L'informazione che la Società riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

a) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate dalla Società in tema di SSL;
b) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di SSL adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale.

Ciò premesso, la Società, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun dipendente, è tenuta ai seguenti oneri informativi:

- deve fornire adeguata informazione ai dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) circa i rischi specifici dell'impresa, per quanto limitati, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- deve essere data evidenza dell'informativa erogata per la gestione del pronto soccorso, emergenza, evacuazione e prevenzione incendi e devono essere verbalizzati gli eventuali incontri;

- i dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) devono ricevere informazione sulla nomina del RSPP, sul Medico Competente e sugli addetti ai compiti specifici per il pronto soccorso, salvataggio, evacuazione e prevenzione incendi;
- deve essere formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Lavoratori;
- il RSPP e/o il Medico Competente devono essere coinvolti nella definizione delle informazioni;
- la Società deve organizzare periodici incontri tra le funzioni preposte alla sicurezza sul lavoro.
- la Società deve coinvolgere il RLS nella organizzazione della attività di rilevazione e valutazione dei rischi, nella designazione degli addetti alla attività di prevenzione incendi, pronto soccorso ed evacuazione.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione.

B - Formazione

- La Società deve fornire adeguata formazione a tutti i dipendenti in materia di sicurezza sul lavoro;
- Il RSPP e/o il Medico Competente devono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione;
- a formazione deve essere adeguata ai rischi della mansione cui il Lavoratore è in concreto assegnato;
- gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso) devono ricevere specifica formazione;
- la società deve effettuare periodiche esercitazioni di evacuazione di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze).

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente.

Comunicazione, flusso informativo e cooperazione

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Società si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori.

A tal proposito la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

a) dal basso verso l'alto

Il flusso dal basso verso l'alto è garantito dalla Società dando la possibilità ai Lavoratori di portare a conoscenza del proprio superiore gerarchico osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale. Inoltre deve essere effettuata verso la sede centrale una reportistica in merito a:

- eventuali incidenti verificatisi;
- azioni implementate al fine di colmare eventuali irregolarità contestate dall'Autorità competente;
- monitoraggio del tasso di incidentalità (con particolare focus sulla diminuzione dello stesso e, se del caso, action plan relativamente a formazione integrativa);
- elenco di ulteriori verifiche / ispezioni da parte dell'ASL / Autorità competenti in materia di igiene, salute e sicurezza sul lavoro.

b) dall'alto verso il basso

Il flusso dall'alto verso il basso ha lo scopo di diffondere a tutti i Lavoratori la conoscenza del sistema adottato dalla Società per la gestione della sicurezza nel luogo di lavoro.

A tale scopo la Società garantisce ai Destinatari un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- eventuali nuovi rischi in materia di salute e sicurezza dei Lavoratori;
- modifiche nella struttura organizzativa adottata dalla Società per la gestione della salute e sicurezza dei Lavoratori;
- contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- ogni altro aspetto inerente alla salute e alla sicurezza dei Lavoratori.

Documentazione

La Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, i seguenti documenti:

- la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro;
- il Documento di Valutazione dei Rischi che indica la metodologia con la quale si è proceduto alla valutazione dei rischi e contiene il programma delle misure di mantenimento e di miglioramento.

La Società è altresì chiamata a garantire che:

- il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente;
- venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente;
- venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;
- vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature ed eventuali dispositivi di protezione individuale forniti dai costruttori;
- venga conservata ogni procedura adottata dalla Società per la gestione della salute e sicurezza sui luoghi di lavoro;
- tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'OdV.

3.4 - I CONTRATTI DI APPALTO

La Società deve predisporre e mantenere aggiornato l'elenco delle aziende che operano sulla base di un contratto d'appalto all'interno dei propri siti. Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espliciti riferimenti agli adempimenti di cui all'art. 26, Decreto Sicurezza, tra questi, in capo al Datore di Lavoro.

3.5 - I CONTROLLI DELL'ODV

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (per le quali si rinvia a quanto esplicitato nella Parte Generale del Modello), l'OdV può:

a) partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
b) accedere a tutta la documentazione aziendale disponibile in materia.

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda.

Inoltre, la Società istituisce altresì a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

A tal proposito, la funzione preposta alla sicurezza (Datore di lavoro ed RSPP) deve informare, nel rispetto della normativa sulla privacy, l'Organismo di Vigilanza periodicamente, e comunque con frequenza almeno semestrale, attraverso uno specifico report, sugli aspetti significativi afferenti le diverse attività di propria competenza, in particolare per quanto attiene a:

- attività di formazione/informazione in tema di sicurezza;
- livelli di incidentalità, con informative specifiche in caso di infortuni con prognosi superiore a 15 giorni;
- contestazioni di violazioni della normativa sulla sicurezza da parte della autorità competente ed esito delle relative prescrizioni;
- documenti di riesame della direzione sul sistema gestionale per la salute e la sicurezza, ove tale sistema sia stato formalmente implementato.

La funzione preposta ha l'obbligo di comunicare immediatamente all'Organismo di Vigilanza ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata.

4. REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Fattispecie di reato.

L'art. 24-bis del Decreto 231 richiama le fattispecie di reato:

- falsità in documenti informatici (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617- quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);

4.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere è emerso che le attività a rischio di commissione dei sopra elencati reati sono le seguenti:

- gestione nomi utenti, password e altri sistemi di sicurezza per l'accesso e l'utilizzo dei sistemi informativi aziendali;
- accesso ed utilizzo della rete aziendale, di internet e della posta elettronica;
- installazione di nuove apparecchiature;
- invio telematico di atti, documenti e scritture.

4.2 - LE ATTIVITÀ DI CONTROLLO

Le Attività di Controllo sui Processi IT – individuati come di pertinenza della LDB Medical Care S.r.L., per il tramite del proprio presidio informatico – sono articolate nelle fasi di seguito descritte e, pur se contestualizzate nell'ambito del rapporto contrattuale "utente-fornitore", svolgono un ruolo integrativo e rafforzativo dell'azione di prevenzione e contrasto dei reati informatici.

In particolare:

1. il Processo di Controllo della gestione della sicurezza fisica e logica è strutturato secondo le seguenti fasi di verifica:
   c) determinazione degli obiettivi e delle strategie di sicurezza informatica attraverso una metodologia di analisi dei rischi in materia di "Information Technology";
   d) accertamento e monitoraggio del corretto e adeguato mantenimento dei livelli di sicurezza stabiliti;
   e) protezione e controllo delle aree fisiche destinate alla gestione dei sistemi informatici, allo scopo di evitare accessi non autorizzati, alterazioni, distrazioni o sottrazioni di "asset" informativi;
   f) identificazione e autenticazione dei codici personali degli utenti necessari ad assicurare "standard" qualitativi per la sicurezza dei dati e delle informazioni e il loro corretto utilizzo;
   g) controlli su un sistema di autorizzazione degli accessi ai dati e alle informazioni, che utilizzi anche tecniche crittografiche e/o di firma digitale per garantire la riservatezza e l'integrità;

2. il Processo di Controllo della prevenzione dalle frodi è strutturato secondo le seguenti fasi di verifica:
   a) previsione di canali e modalità di comunicazione per la segnalazione tempestiva di incidenti e situazioni sospette allo scopo di minimizzare i rischi e i danni generati e poter prevenire comportamenti irregolari, anomali o inadeguati
   b) interventi e forme di raccordo con il "gestore del sistema" per la disciplina delle modalità di comunicazione alle Forze dell'Ordine e alle Autorità pubbliche di controllo;

3. il Processo di Controllo della gestione della "progettazione & sviluppo" e dell'attivazione & supporto dei servizi IT è strutturato secondo le seguenti fasi di verifica:
   a) previsione della separazione degli ambienti informatici di sviluppo, collaudo e produzione nei quali i sistemi e le applicazioni vengono installati, gestiti e manutenuti;
   b) predisposizione e conservazione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionali al sicuro e corretto svolgimento delle attività informatiche;
   c) accertamento e monitoraggio sugli interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti ovvero sostituiti da nuove "release" aggiornate;
   d) controlli su procedure di pianificazione e gestione dei salvataggi di sistemi operativi, "software", dati e informazioni, configurazioni di sistema;
   e) monitoraggio sulla gestione degli strumenti di "hardware" e di ogni "asset" informatico in dotazione, anche attraverso la definizione "standard" di custodia, utilizzo, riproduzione,

distruzione e trasposto fisico dei supporti rimovibili e dei PC per proteggerli da danneggiamenti, furti e usi non autorizzati;

f) accertamento e controllo della tracciabilità dei processi decisori, anche ai fini di archiviazione e conservazione dei documenti inerenti agli "iter"decisionali, riguardanti le fasi di progettazione, sviluppo, manutenzione o cambiamento di sistemi, applicazioni e reti IT.

4. il Processo di Controllo della gestione della protezione dei dati e delle informazioni è strutturato secondo le seguenti fasi di verifica:
   a) accertamento e monitoraggio tramite "check-list" e altri tabulati, rilasciati o resi disponibili dal "gestore del sistema", per controllare i profili di accesso, in ragione dei ruoli e delle funzioni esercitati all'interno delle diverse componenti societarie, organizzative e funzionali della Medical Care S.r.L.;
   b) presidio delle contromisure individuate per la protezione dei dati gestiti dai sistemi informativi nel rispetto dei requisiti di riservatezza, integrità e disponibilità informativa, stabiliti in funzione degli ambiti e delle modalità di utilizzo dalle disposizioni di legge o dalla normativa interna e secondaria emanata dalle Autorità pubbliche di controllo;
   c) previsione di misure di sicurezza delle applicazioni informatiche in termini di istallazione, gestione dell'esercizio e delle emergenze, protezione dei codici, che assicurino la preservazione dei requisiti di "privacy", integrità e disponibilità delle informazioni e dei dati trattati;
   d) prevenzione da software dannosi, mediante l'adozione di strumenti e infrastrutture tecnologiche adeguate, che prevedano l'utilizzo e la diffusione di sistemi antivirus e modalità sicure per lo scambio e l'acquisizione delle informazioni e dei dati tramite "e-mail" e connessioni ai siti "web".

4.3 - LE PROCEDURE SPECIFICHE

Al fine di mitigare il rischio di commissione dei Delitti Informatici e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, assolve i seguenti adempimenti:

- fornisce ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli user-id e delle password per accedere ai principali sottosistemi informatici utilizzati;
- limita, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
- effettua, per quanto possibile, nel rispetto della normativa sulla privacy e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

4.4 - REGOLE DI COMPORTAMENTO

Obiettivo della presente Parte Speciale è che tutti i Destinatari del Modello si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei delitti informatici. Nell'espletamento delle attività aziendali e, in particolare, nell'ambito delle attività a rischio di commissione dei reati, è espressamente vietato, anche in relazione al tipo di rapporto posto in essere con la Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o

collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (art. 24-bis Decreto).

In particolare non è ammesso:

- porre in essere quei comportamenti che integrano le fattispecie di reato o, sebbene non costituiscano di per sé un'ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo);
- divulgare informazioni relative ai sistemi informatici aziendali;
- utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta.

Ai fini dell'attuazione delle regole e del rispetto dei divieti elencati, devono essere ottemperati i principi procedurali qui di seguito descritti, oltre alle Regole e ai Principi Generali già contenuti nella Parte Generale del presente Modello:

1. i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati;
2. è vietato introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato;
3. è vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili;
4. è vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
5. è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;
6. è vietato divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
7. è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
8. è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
9. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
10. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;
11. è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
12. è vietato comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
13. è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati.

4.5 - I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale del Modello, relativamente ai suoi poteri e doveri ivi compreso quello, discrezionale, di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività

potenzialmente a rischio diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Società. L'Organismo di Vigilanza dovrà esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.

5. REATI AMBIENTALI

Fattispecie di reato.

L'art. 25-undecies del Decreto 231 richiama le fattispecie di reato:

- Attività di gestione di rifiuti non autorizzata (articolo 256, D.Lgs. n. 152/2006).

5.1 - LE ATTIVITÀ A RISCHIO

Con riferimento alle fattispecie disciplinate dall'art. 25-undecies del D.Lgs. 231/01, sono state individuate le principali aree a rischio reato in cui l'azienda potrebbe essere coinvolta e le attività da ritenersi maggiormente "sensibili", ossia quelle attività il cui svolgimento espone la Società al rischio di commissione dei reati individuati nell'ambito della normativa di riferimento.

La raccolta dei campioni biologici deve avvenire adottando precauzioni e dispositivi di protezione individuale utili a minimizzare la possibilità di esposizione a patogeni.

Di seguito, si riportano le attività per l'area a rischio reato riferita alla gestione della raccolta e smaltimento di rifiuti pericolosi:

- attività di identificazione, caratterizzazione e classificazione dei rifiuti;
- attività di raccolta e deposito temporaneo dei rifiuti;
- selezione e gestione dei fornitori per l'attività di raccolta, trasporto e smaltimento dei rifiuti.

Tali fattispecie potrebbe verificarsi in caso di scorretto smaltimento dei rifiuti medico sanitari derivanti sia dalle attività di prelievo campioni.

5.2 - LE PROCEDURE SPECIFICHE

Organi e funzioni aziendali coinvolte In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti i seguenti organi e funzioni aziendali:

- Medici, Infermieri, OSS e altri specialisti medici regolarmente iscritti all'albo professionale di riferimento, in servizio esterno alla LDB Medical Care S.r.L., addetti al prelievo.

Tutte le attività che comportano il pericolo di esposizione ad agenti biologici debbono essere svolte attuando le misure tecniche, organizzative e procedurali per eliminare o ridurre al minimo il rischio di esposizione.

Lo norme di riferimento sono quelle stabilite dal D.Lgs. 81/08 Allegato XLVI.

I rifiuti potenzialmente contaminati devono essere trattati ed eliminati come materiale infetto categoria B (UN3291).

Procedure da attuare:

Tra le regole e procedure che prevedono le modalità per lo svolgimento delle attività necessarie a mitigare i fattori di rischio caratteristici delle aree a rischio identificate ed i relativi controlli, si elencano:

- l'esistenza di un processo di gestione dell'affidamento dei compiti specifici ai lavoratori in tema di ambiente;
- la scelta di fornitori di servizi ambientali in base alla relativa competenza e professionalità, oltre che al possesso delle necessarie autorizzazioni di legge;

- l'aggiornamento delle informazioni riguardo alla legislazione rilevante per le tematiche ambientali, ivi inclusi i criteri e le modalità per la comunicazione di tali aggiornamenti alle funzioni aziendali interessate;
- la gestione delle emergenze ambientali, ivi inclusi il recepimento dei miglioramenti tecnologici del settore e le modalità e la tempistica/frequenza di svolgimento delle esercitazioni di emergenza;
- l'identificazione e valutazione dei rischi ambientali, nonché l'identificazione degli aspetti ambientali e valutazione della loro significatività in funzione degli impatti ambientali diretti e indiretti ad essi correlati, per servizi resi e attività svolte in condizioni operative normali e anomale;
- la gestione della raccolta e consegna dei rifiuti medico-sanitari che prevede:
  a) le modalità di raccolta dei rifiuti e l'identificazione dei contenitori idonei al loro trasporto e smaltimento;
  b) le modalità di consegna al service esterno, responsabile dello smaltimento dei rifiuti.
- la gestione della documentazione relativa al sistema di controllo per le tematiche ambientali (ivi compresa l'archiviazione e la conservazione);
- la gestione della diffusione periodica verso i lavoratori, da parte delle funzioni competenti, delle informazioni connesse alla normativa vigente relativa all'ambiente;
- la gestione del processo di formazione del personale in materia ambientale.

In particolare:

- adottare le misure per prevenire o ridurre al minimo la propagazione accidentale all'esterno dell'area di lavoro;
- esporre in modo chiaro e visibile il segnale di rischio biologico;
- mettere in atto le procedure idonee per il trasporto dei campioni:
  - trattare tutti i campioni prelevati come potenzialmente pericolosi o a rischio infettivo indossando guanti monouso;
  - assicurare la corretta chiusura, etichettatura e identificazione del contenitore primario (provetta);
  - porre i campioni in una rastrelliera;
  - alloggiare la rastrelliera in un contenitore secondario dotato di sistema di chiusura;
  - assicurare alloggiamento al di fuori del contenitore secondario della documentazione di accompagnamento dei campioni biologici;
- definire le procedure di emergenza in caso di incidente: in caso di caduta accidentale di provette (contenitori primari) e contenitori secondari destinati al trasporto, con conseguente rottura e/o spandimento di liquidi biologici, è indispensabile un intervento di bonifica ambientale immediato:
  - indossare guanti in gomma (nel caso ci siano frammenti di vetro) e, se necessario, soprascarpe, mascherina, e schermo protettivo;
  - coprire lo spandimento con fogli assorbenti appositi/carta assorbente imbevuti di disinfettante a base di ipoclorito di sodio, ovvero, nel caso di superfici metalliche, utilizzare disinfettante a base di polifenoli;
  - rimuovere il materiale utilizzando attrezzi adeguati (pinze, scopino e paletta);
  - non rimuovere il materiale con le mani, anche se protette da guanti;
  - smaltire i frammenti di vetro nel contenitore rigido apposito per taglienti (ago-box);
  - smaltire il restante materiale come rifiuto pericoloso a rischio infettivo nei contenitori per Rifiuti Ospedalieri Trattati (ROT);

  - successivamente lavare l'area con specifico detergente/disinfettante per bonifica ambientale; lasciare agire il detergente/disinfettante per il tempo indicato;
- evitare l'utilizzo di contenitori non idonei e/o sprovvisti di indicazione del contenuto;
- adottare idonee misure igieniche: il lavaggio frequente delle mani è riconosciuto come la più importante misura per ridurre il rischio di trasmissione di microrganismi da una persona all'altra o da una localizzazione all'altra nello stesso paziente. Lavarsi le mani è un'operazione semplice, ma deve avvenire secondo precise regole. Il lavaggio sociale e/o antisettico prevede le seguenti azioni:
  - insaponare le mani accuratamente (dita, palmo, dorso, polsi, unghie) per almeno 10 secondi e sciacquare con acqua corrente in modo completo;
  - in caso di imbrattamento con liquidi organici, procedere al lavaggio con acqua e sapone per almeno 30 secondi seguito da antisepsi (con prodotti a base di Clorexidina 4%, PVP-J) in modo completo, risciacquo con acqua corrente, e asciugatura con salviette in carta monouso;
- adottare idonei dispositivi di protezione individuale che devono essere sottoposti a verifica, puliti e disinfettati al termine di ogni ciclo lavorativo:
  - i DPI per il rischio biologico devono possedere marcatura CE come dispositivo di protezione individuale in III categoria secondo il Regolamento (UE) 2016/425 in vigore dal 21 aprile 2018 - D.lgs 17/2019 contenente "Adeguamento della normativa nazionale alle disposizioni del Regolamento UE n. 2016/425 sui DPI"), ed essere corredati da note informative sul loro impiego e manutenzione (rif. D.Lgs. 81/08 Titolo III; INAIL 2011);
  - i guanti per la protezione da microorganismi devono essere conformi alla norma tecnica EN 374:2003;
  - dispositivi di protezione del corpo come camici, tute, copri-camice impermeabili, ecc. non sono in genere considerati DPI ma indumenti protettivi, in quanto non proteggono da specifici rischi; diversamente appartengono ai DPI monouso specifici camici impermeabili e tute in tessuto non tessuto a protezione totale del corpo; gli indumenti per la protezione contro gli agenti infettivi devono essere conformi alla norma tecnica EN 14126:2003;
- deve essere tassativamente vietato fumare, ed assumere cibi e bevande nel trasporto dei materiali biologici;
- nel caso di incidenti che possono provocare dispersione nell'ambiente di agenti biologici appartenenti ai gruppi II e III, gli addetti debbono abbandonare immediatamente l'area e deve essere effettuata contestualmente la segnalazione dell'evento alla ASL competente territorialmente in ordine alle cause che lo hanno determinato, ed alle misure adottate, ovvero da adottare, per la bonifica del luogo dell'incidente;
- nelle attività che presentano un pericolo da agenti biologici, gli addetti debbono essere adeguatamente informati e formati, in particolare in ordine a:
  - rischi per la salute dovuti agli agenti utilizzati;
  - precauzioni da prendere per evitare l'esposizione;
  - misure igieniche da osservare;
  - funzione ed il corretto utilizzo dei DPI e degli indumenti da lavoro;
  - procedure atte a prevenire il verificarsi di infortuni;
  - misure da adottare per ridurre al minimo le conseguenze in caso di infortuni.

Per quanto attiene all'esecuzione di tampone oro-nasofaringeo per COVID 19:

- i campioni usati all'interno delle strutture ove si svolge il servizio, sono smaltiti come rifiuti e custoditi in apposito contenitore a norma di legge per il trasporto di campioni biologici, da consegnare alla Società di servizi responsabile del trattamento.
- sono disponibili procedure aziendali per l'esecuzione dei tamponi.

Per quanto attiene all'esecuzione di prelievo venoso per test sierologici per COVID-19 e non:

- l'esecuzione della procedura per il prelievo venoso avviene nel pieno rispetto delle raccomandazioni della Società Italiana di Biochimica Clinica e Biologia Molecolare Clinica - Medicina di Laboratorio (SiBioC) e della Società Italiana di Patologia Clinica e Medicina di Laboratorio (SiMeL).
- sono previste procedure aziendali per l'esecuzione dei prelievi venosi, COVID o per analisi ematochimiche generiche.

Sono altresì disponibili le procedure aziendali per la Determinazione delle Sostanze d'Abuso.

Per quanto attiene la trattazione e il trasporto dei campioni biologici prelevati nelle strutture ove si svolge il servizio, la società ha in essere un contratto di service con la società BIOS San Giovanni.

Sono disponibili le procedure di trasporto a carico e sotto la responsabilità diretta della BIOS San Giovanni.

5.3 - REGOLE DI COMPORTAMENTO

La presente Parte Speciale è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a rischio reato e nello svolgimento delle attività sensibili.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale del Modello, in linea generale e al fine di perseguire la prevenzione dei reati ambientali è fatto espresso divieto a tutti i soggetti destinatari di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-undecies del D.Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale.

È da considerarsi vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplata dall'art. 25-undecies del D.Lgs. 231/01.

Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (Sistema di Deleghe, Codice Etico, ecc.), gli organi sociali, gli amministratori, i dipendenti aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nelle svolgimento delle attività a rischio, **sono tenuti,** al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25-undecies del D.Lgs. 231/01, al rispetto delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio.

5.4 - I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale del Modello relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'OdV effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale.

Tali controlli sono diretti a verificare la corretta applicazione dei principi e delle regole generali di comportamento del presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

Inoltre, i compiti di vigilanza dell'OdV in relazione all'osservanza del Modello, per quanto concerne i reati di cui alla presente Parte Speciale, si esplicano anche nel:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati ambientali;
- monitorare sul rispetto delle procedure interne per la prevenzione dei suddetti reati monitoraggio specifico sulle attività sensibili dell'azienda che la espongono ai reati esaminati nella presente Parte Speciale;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente dell'azienda ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

6. REATI CONTRO LA PERSONALITÀ INDIVIDUALE

Fattispecie di reato.

L'art. 25-quinquies del Decreto 231 richiama le fattispecie di reato:

- riduzione o mantenimento in schiavitù o servitù (art. 600 c.p.);
- prostituzione minorile (art. 600-bis c.p.);
- pornografia minorile (art. 600-ter c.p.);
- detenzione di materiale pornografico (art. 600-quater c.p.);
- pornografia virtuale (art. 600-quater .1 c.p.);
- iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.);
- tratta di persone (art. 601 c.p.);
- acquisto e alienazione di schiavi (art. 602 c.p.).

6.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere e dalle risposte fornite in sede di intervista, è emerso che l'attività a rischio di commissione dei sopra elencati reati è riferibile alla **gestione delle assunzioni.**

6.2 - LE PROCEDURE SPECIFICHE

Tutte le aree aziendali devono osservare l'apposita procedura che disciplina le modalità operative per la gestione delle assunzioni.

6.3 - REGOLE DI COMPORTAMENTO

E' fatto espressamente divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-quinquies, D.Lgs. 231/2001);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possono potenzialmente diventarlo.

6.4 - I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale del Modello, relativamente ai suoi poteri e doveri ivi compreso quello, discrezionale, di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'OdV effettua periodicamente controlli sulle attività potenzialmente a rischio diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Società.

L'Organismo di Vigilanza dovrà esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.

Inoltre, i compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i reati contro la personalità individuale sono i seguenti:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

7. RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA

Fattispecie di reato.

L'art. 25-octies del Decreto 231 richiama le fattispecie di reato:

- ricettazione (art. 648 c.p.);
- riciclaggio (art. 648 bis c.p.);
- impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);

7.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere e dalle risposte fornite in sede di intervista, è emerso che l'attività a rischio di commissione dei suddetti reati è riferibile alla **gestione dei flussi finanziari.**

7.2 - LE PROCEDURE SPECIFICHE

Tutti i pagamenti effettuati a favore della Società devono essere effettuati a mezzo di bonifico bancario o tramite assegno intestato alla Società.

7.3 - REGOLE DI COMPORTAMENTO

I Destinatari dovranno, inoltre, attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai Reati di Riciclaggio;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/partner anche stranieri;
4. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della

liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
5. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
6. effettuare un costante monitoraggio dei flussi finanziari aziendali.

7.4 - I CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo. In particolare, è compito dell'Organismo di Vigilanza:

a) monitorare l'efficacia delle procedure interne per la prevenzione dei Reati di Riciclaggio;
b) proporre eventuali modifiche nelle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
c) esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi esponente della Società ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

L'Organismo di Vigilanza svolge altresì un ruolo attivo e propositivo nella formulazione di adeguati programmi e procedure.

8. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

Fattispecie di reato.

L'art. 25-novies del Decreto 231 richiama le fattispecie di reato:

- tutte le fattispecie delittuose di cui agli artt. 171, primo comma, lettera a-bis e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della Legge 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

8.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere e dalle risposte fornite in sede di intervista, è emerso che le attività a rischio di commissione dei sopra elencati reati sono le seguenti.

- attività di presentazione dell'azienda al pubblico, anche attraverso l'ausilio di consulenti;
- attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altra opera dell'ingegno tutelata dal diritto d'autore.

8.2 - LE PROCEDURE SPECIFICHE

Tutti i Destinatari che svolgono la loro attività nelle aree a rischio reato sono tenuti al rigoroso rispetto della procedura controllo dei fornitori, nonché di tutte quelle ulteriori procedure che la Società eventualmente predisporrà in seguito, in ottemperanza ad esigenze aziendali e/o normative.

8.3 - REGOLE DI COMPORTAMENTO

Obiettivo della presente Parte Speciale è conformare le regole di condotta a tutti i destinatari, al fine di prevenire e impedire il verificarsi dei reati contro il diritto d'autore. Nell'espletamento delle attività aziendali e, in particolare, nell'ambito delle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi

individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate dall'art 25-novies del Decreto.

8.4 - I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale del Modello, l'OdV effettua periodicamente controlli sulle attività potenzialmente a rischio diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Società. L'Organismo di Vigilanza dovrà esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni. Inoltre, i compiti di vigilanza dell'OdV in relazione all'osservanza del Modello, per quanto concerne i reati contro il diritto d'autore, sono i seguenti:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- monitoraggio sul rispetto delle procedure interne per la prevenzione dei reati contro il diritto d'autore. L'OdV è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

9. REATI DI CRIMINALITÀ ORGANIZZATA

Fattispecie di reato.

L'art. 24-ter del Decreto 231 richiama le fattispecie di reato:

- delitti di criminalità organizzata (art. 24-ter, D.Lgs. 231/01);
- associazione per delinquere (art. 416 c.p.);
- delitti di associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, 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.);
- associazioni di tipo mafioso anche straniere (art. 416-bis c.p.);
- scambio elettorale politico-mafioso (art. 416-ter c.p.);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR. 9 ottobre 1990, n. 309);
- produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope (art. art. 73 DPR. 9 ottobre 1990, n. 309);
- sequestro di persona a scopo di rapina o di estorsione (art. 630c.p.);
- delitti concernenti la fabbricazione ed il traffico di armi da guerra, esplosivi ed armi clandestine (art. 407 comma 2 lettera a c.p.p).

9.1 - LE ATTIVITÀ A RISCHIO

Dall'analisi delle procedure in essere e dalle risposte fornite in sede di intervista, è emerso che le attività a rischio di commissione dei sopra elencati reati riferibili alla **gestione degli appalti di lavori, servizi e forniture.**

9.2 - REGOLE DI COMPORTAMENTO

E' fatto espressamente divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-bis1, D.lgs. 231/2001); porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possono potenzialmente diventarlo.

9.3 - I CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV effettua controlli periodici diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e delle procedure aziendali cui la stessa fa esplicito o implicito richiamo. In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia delle procedure interne per la prevenzione dei reati di criminalità organizzata;
- proporre eventuali modifiche nelle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi esponente della Società ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante. Di ogni riunione deve redigersi apposito processo verbale, sottoscritto dagli intervenuti.