SYSTEM MANAGEMENT S.P.A.

Modello di Organizzazione(*ex* d.lgs. 231/2001)
Ultimo aggiornamento novembre 2022

System Management

Sommario

1. PREMESSA

Il presente documento viene redatto ai sensi di quanto previsto:

- dalla Convenzione di Bruxelles del 26 luglio 1995 sulla protezione degli interessi finanziari della Comunità Economica Europea;
- dalla Convenzione di Bruxelles del 26 maggio 1997 sulla lotta contro la corruzione dei pubblici ufficiali nell'ambito della Comunità Economica Europea e degli Stati Membri;
- dalla Convenzione OECD del 21 novembre 1997 per la lotta contro la corruzione dei pubblici ufficiali esteri nelle transazioni internazionali;
- dal decreto legislativo n. 231/2001 così come emanato e integrato dalla successiva legislazione (in seguito, "il Decreto"), in particolare per individuare un modello di organizzazione societaria finalizzato alla prevenzione dei reati individuati nel Decreto enelle Convenzioni;
- dalle Linee Guida di Confindustria del 7 marzo 2002, del marzo 2014 ed aggiornate al giugno2021;
- dal D.Lgs. 75/2020 che ha introdotto nuove fattispecie di reato, una nuova valutazione del rischiodi commissione dei reati presupposto riconducibili alla società con riferimento ai reati tributari e a quelli di contrabbando.

Con la L. 16 marzo 2006, n. 146 di ratifica ed esecuzione della Convenzione e dei protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, sono stati introdotti alcuni reati aventi rilevanza ai sensi del Decreto qualora siano attuati da un Gruppo criminale organizzato e aventi il carattere di *transnazionalità*, con tale dicitura intendendo la necessità che questi siano commessi:

1. in più di uno Stato;
2. in uno Stato purché, però, una parte sostanziale della loro preparazione, pianificazione, direzione o controllo sia avvenuta in un altro Stato;
3. in uno Stato ma in essi deve risultare implicato un gruppo criminale organizzato, impegnato in attività criminali in più di uno Stato;
4. in uno Stato ma con effetti sostanziali in un altro Stato.

In particolare, non interessa, ai fini del D.Lgs. 231/2001, il reato occasionalmente transnazionale; ciò che interessa la norma è rappresentato da quel reato frutto di una attività organizzata dotata di stabilità e

prospettiva strategica e suscettibile di essere ripetuto nel tempo.

2. STRUTTURA DEL DOCUMENTO

Il presente documento è composto da una Parte Generale e una Parte Speciale.
La Parte Generale descrive: la disciplina contenuta nel d.lgs. 231/2001 ed i reati rilevanti per la Società, indicai destinatari del Modello ed i principi di funzionamento dell'Organismo di Vigilanza, definisce un sistema sanzionatorio dedicato al presidio delle violazioni del Modello, gli obblighi di comunicazione dello stesso e di formazione del personale.
La Parte Speciale ha ad oggetto l'indicazione delle attività "sensibili" – cioè delle attività che sono state considerate dalla Società a rischio di reato, in esito alle analisi dei rischi condotte – ai sensi del Decreto, i principi generali di comportamento, gli elementi di prevenzione a presidio delle suddette attività e le misuredi controllo essenziali deputate alla prevenzione o alla mitigazione degli illeciti.
Costituiscono inoltre parte integrante del Modello:

- il Codice Etico, che definisce i principi e le norme di comportamento della Società;
- Il Codice Sanzionatorio.

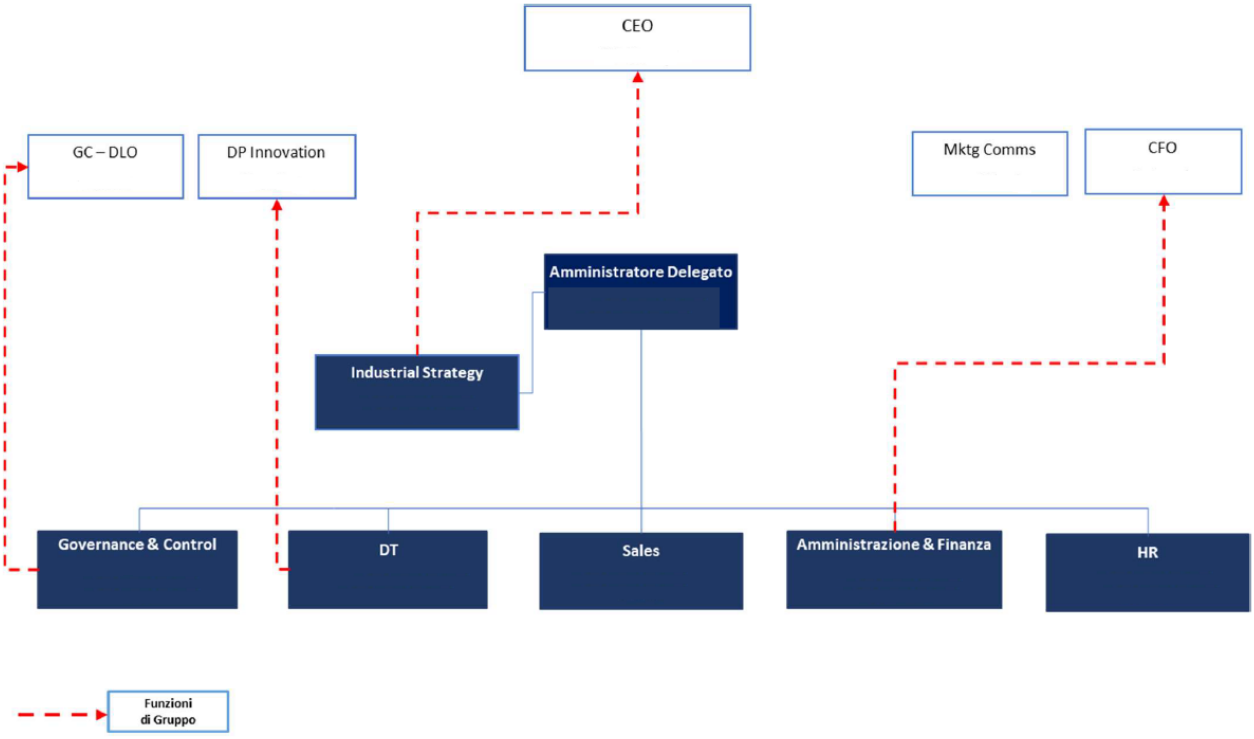
Tutte le disposizioni, i provvedimenti interni, gli atti e le procedure operative aziendali che del presente documento costituiscono attuazione (ad esempio statuto, poteri, organigrammi, *job description*, procedure) sono reperibili secondo le modalità previste per la loro diffusione all'interno dell'azienda.

System Management

PARTE GENERALE

1. LA SOCIETA'

La Società System Management S.P.A. (d'ora innanzi anche indicata come la Società) opera a livello nazionale nel campo della produzione, commercializzazione, installazione e manutenzione di sistemi informatici e delle reti, nonché la produzione e commercializzazione di software specialistico di ambiente applicativo.
La società ha sede legale in Napoli e uffici operativi in Roma e Milano.
La clientela della Società è composta sia da primarie aziende private che da amministrazioni ed enti pubblici.



2. IL CONTESTO NORMATIVO DI RIFERIMENTO

2.1 La disciplina della responsabilità amministrativa

Il decreto legislativo 8 giugno 2001 n. 231 "*Disciplina della responsabilità amministrativa delle persone giuridiche delle società e delle associazioni anche prive di personalità giuridica*", in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 3001, ha introdotto la "*responsabilità degli enti per gli illeciti amministrativi dipendenti da reato*" che si applica sia agli enti dotati di personalità giuridica sia alle società ed associazioni prive di personalità giuridica.
Tale responsabilità amministrativa degli enti si aggiunge alla responsabilità penale della persona fisica che ha commesso il reato.
Secondo la disciplina introdotta dal Decreto, infatti, gli enti possono essere ritenuti responsabili per alcuni reati commessi o tentati, **nell'interesse o a vantaggio degli stessi**, da esponenti dei vertici aziendali, in **posizione apicale, e/o da coloro che sono sottoposti alla direzione o vigilanza dei primi** (art. 5, comma 1, del d.lgs. n. 231/2001). Nei casi di cui sopra gli enti stessi sono soggetti, in via diretta ed autonoma, a determinate sanzioni amministrative. Così recita, infatti, l'art. 5, comma 1, del d.lgs. n. 231/2001: "Responsabilità della società – *La società è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità*

organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto,la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)".

Gli autori del reato possono quindi essere:

a) soggetti con funzioni di amministrazione, gestione e direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché coloro che esercitano, anche solo di fatto, la gestione ed il controllo dell'Ente (cd. **soggetti in posizione apicale**), e dunque, persone che rivestono funzioni di rappresentanza, di amministrazione o direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale e che svolgono, anche di fatto, la gestione e il controllo dell'Ente stesso. Si tratta di soggetti che, in considerazione delle funzioni che svolgono, vengono denominati "apicali". In particolare, nella categoria dei soggetti apicali (a) possono essere fatti rientrare gli amministratori, i direttori generali, i rappresentanti legali, ma anche, per esempio, i direttori e i responsabili di area. Tutti i soggetti delegati dagli amministratori a esercitare attività di gestione o direzione della Società devono essere considerati soggetti apicali;

b) soggetti sottoposti alla direzione e al controllo da parte dei soggetti apicali (cd. **soggetti sottoposti**). Alla categoria dei soggetti in posizione subordinata appartengono tutti coloro che sono sottoposti alla direzione e vigilanza dei soggetti apicali e che, in sostanza, eseguono le decisioni adottate dai vertici. Possono essere ricondotti a questa categoria tutti i dipendenti dell'Ente, nonché tutti coloro che agiscono in nome, per conto o nell'interesse dell'Ente, quali, a titolo di esempio, i collaboratori e i consulenti, nonché i responsabili di processo.

Tale responsabilità mira sostanzialmente a coinvolgere nella sanzione di determinati illeciti il patrimonio degli enti coinvolti e, in ultima analisi, gli interessi economici dei soci della società, i quali, fino all'entrata in vigore del decreto in esame, non erano soggetti a conseguenze dirette dalla realizzazione di reati commessi nell'interesse o a vantaggio della propria società.

Circa il concetto di interesse occorre che il medesimo sussista qualora il soggetto qualificato abbia agito, fraudolentemente, per un vantaggio proprio o di terzi e dell'impresa anche se questo, per l'Ente, sia parziale o marginale. Dunque, il concetto di interesse assume un'indole soggettiva riferendosi alla sfera volitiva della persona fisica che agisce e valutando il proprio comportamento al momento della condotta.

L'interesse, di recente, deve essere letto anche in chiave oggettiva valorizzando la componente finalistica della condotta.

Con riferimento al vantaggio si rileva come il medesimo si debba caratterizzare come complesso di benefici – prevalentemente di carattere patrimoniale – tratti dal reato. Il vantaggio, contrariamente all'interesse, può valutarsi *ex post* alla commissione della condotta fraudolenta . Il vantaggio "patrimoniale" può essere inteso anche in termini di risparmio di spesa.

Nei reati colposi, tra cui sicurezza sul lavoro (art. 25 septies) e ambiente (art. 25 undecies), l'interesse e il vantaggio debbono, prevalentemente, riferirsi alla condotta inosservante delle norme cautelari .

Dalla sua entrata in vigore, il decreto 231 ha subito continui aggiornamenti normativi relativi alle fattispeciedi reato.

Di seguito si riportano i principali aggiornamenti e l'elenco aggiornato del catalogo dei reati presupposto:

- reati commessi nei rapporti con la Pubblica Amministrazione, artt. 24 (Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture) e art. 25 (Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio) del d.lgs. n. 231/2001;
- delitti informatici e trattamento illecito dei dati, introdotti dall'articolo 7 della L. 18 marzo 2008, n. 48, che ha inserito nel d.lgs. n. 231/2001 l'art. 24bis;
- delitti di criminalità organizzata, introdotti dall'art. 2, comma 29, della L. 15 luglio 2009, n. 94, che ha inserito nel d.lgs. n. 231/2001 l'art. 24ter;
- reati in tema di falsità in monete, carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento, introdotti dall'art. 6 della L. 23 novembre 2001, n. 409, che ha inserito nel d.lgs. n. 231/2001 l'art. 25bis, come modificato dall'articolo 15, comma 7, lett. a), della L. 23 luglio 2009, n. 99;
- delitti contro l'industria e il commercio, introdotti dall'art. 15, comma 7, lett. b), della L. 23 luglio 2009,

n. 99, che ha inserito nel d.lgs. n. 231/2001 l'art. 25bis.1;

- reati societari, introdotti dal d.lgs. 11 aprile 2002, n. 61, che ha inserito nel d.lgs. n. 231/2001 l'art. 25ter, modificato dalla L. 6 novembre 2012, n. 190 e, successivamente, dal d.lgs. 15 marzo 2017, n. 38;
- delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, introdotti dalla Legge 14 gennaio 2003, n. 7, che ha inserito nel d.lgs. n. 231/2001 l'articolo 25quater;
- delitti di pratiche di mutilazione degli organi genitali femminili, introdotti dalla L. 9 gennaio 2006, n. 7, che ha inserito nel d.lgs. n. 231/2001 l'articolo 25quater.1;
- delitti contro la personalità individuale, introdotti dalla L. 11 agosto 2003, n. 228, che ha inserito nel d.lgs. n. 231/2001 l'art. 25quinquies, successivamente modificato dall'articolo 10 della L. 6 febbraio 2006, n. 38 e dalla L. n. 199/2016;
- reati di abuso di informazioni privilegiate e di manipolazione del mercato, previsti dalla L. 18 aprile 2005, n. 62, che ha inserito nel d.lgs. n. 231/2001 l'art. 25sexies;
- reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e sicurezza dei lavoratori, introdotti dalla L. 3 agosto 2007, n. 123, che ha inserito nel d.lgs. n. 231/2001 l'art. 25septies, come modificato dall'art. 300 del d.lgs. 9 aprile 2008, n. 81;
- reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, introdotti dal d.lgs. 21 novembre 2007, n. 231, che ha inserito nel d.lgs. n. 231/2001 l'art. 25octies, poi modificato dalla L. 186/2014 e da ultimo sostituito dall'articolo 72, comma 3, del d.lgs. 21 novembre 2007, n. 231, come modificato dall'articolo 5, comma 1, del d.lgs. 25 maggio 2017, n. 90;
- delitti in materia di strumenti di pagamento diversi dai contanti, aggiunto dal d.lgs. 184/2021;
- delitti in materia di violazione del diritto d'autore, introdotti dall'art. 15, comma 7, lett. c), della L. 23 luglio 2009, n. 99, che ha inserito nel d.lgs. n. 231/2001 l'art. 25novies;
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dall'art. 4 della L. 3 agosto 2009, n. 116, come sostituito dall'art. 2, co. 1, d.lgs. 7 luglio 2011, n. 121, che ha inserito nel d.lgs. n. 231/2001 l'art. 25decies;
- reati ambientali, introdotti dall'art. 4, co. 2, L. 3 agosto 2009, n.116, come sostituito dall'art. 2, co. 1, d.lgs. 7 luglio 2011, n. 121, che ha inserito nel d.lgs. n. 231/2001 l'art. 25undecies, successivamente aggiornato dalla Legge 68/2015 e modificato dal d.lgs. 21/2018;
- reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, introdotto dall'art. 2 del d.lgs. 16 luglio 2012, n. 109, che ha inserito nel d.lgs. n. 231/2001 l'art. 25duodecies, modificato dalla Legge 161/2017;
- reati in materia di razzismo e xenofobia, introdotti dalla L. 20 novembre 2017, n. 167, che ha inserito nel d.lgs. n. 231/2001 l'art. 25terdecies, poi modificato dal d.lgs. 21/2018;
- reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, introdotti dalla L. del 3 maggio 2019 n. 39 che ha inserito nel d.lgs. n. 231/01 l'art. 25quartedecies;
- reati tributari, introdotti dal D.l. del 26 ottobre 2019, n. 124, convertito con L. 157/2019, che ha inserito nel d.lgs. n. 231/01 l'art. 25 quinquiesdecies, poi modificato dal d.lgs. 75/2020;
- reati di contrabbando, introdotti dal d.lgs.75/2020 che ha inserito nel d.lgs. 231/01 l'art. 25 sexiesdecies;
- reati contro il patrimonio culturale, a seguito dell'approvazione del DDL 14 dicembre 2021, n. 882, il cui testo ha previsto l'inserimento delle fattispecie incriminatrici di cui al Codice dei beni culturali (D.Lgs. 42/2004) nel Codice Penale. In particolare, sono stati previsti due nuovi articoli nel catalogo del d.lgs. 231/01: l'art. 25 septiesdecies rubricato "Delitti contro il patrimonio culturale" che prevede sanzioni pecuniarie e interdittive per i delitti in materia di alienazione, appropriazione indebita, importazione illecita, uscita o esportazione illecite, distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici, contraffazione di opere d'arte, furto, ricettazione di beni culturali e falsificazione in scrittura privata relativa a beni culturali; l'art. 25 duodevicies rubricato "Riciclaggio di beni culturali e devastazione e saccheggio di beni

culturali e paesaggistici" che allarga la responsabilità della persona giuridica ai reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici.

Con la L. 16 marzo 2006, n. 146 di ratifica ed esecuzione della Convenzione e dei protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, sono stati introdotti alcuni reati aventi rilevanza ai sensi del Decreto qualora siano posti in essere da un Gruppo criminale organizzato e aventi il carattere di transnazionalità, con tale dicitura intendendo la necessità che questi siano commessi:

1. in più di uno Stato;
2. in uno Stato purché, però, una parte sostanziale della loro preparazione, pianificazione, direzione o controllo sia avvenuta in un altro Stato;
3. in uno Stato ma in essi deve risultare implicato un gruppo criminale organizzato, impegnato in attività criminali in più di uno Stato;
4. in uno Stato ma con effetti sostanziali in un altro Stato.

In particolare, non interessa, ai fini del D.Lgs. 231/2001, il reato occasionalmente transnazionale; ciò che interessa la norma è rappresentato da quel reato frutto di una attività organizzata dotata di stabilità e prospettiva strategica e suscettibile di essere ripetuto nel tempo. La responsabilità ex d.lgs. 231/2001 di un ente può realizzarsi quando i reati di seguito indicati si attuano, nell'interesse o a vantaggio dell'Ente stesso, attraverso contatti con una realtà criminale organizzata:

- disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D.Lgs. 25 luglio 1998, n. 286);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309);
- associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- favoreggiamento personale (art. 378 c.p.);
- associazione per delinquere (art. 416 c.p.);
- associazione di tipo mafioso (art. 416-bis c.p.).

La normativa del D.Lgs. 231/01 ha registrato modifiche ed evoluzioni anche in merito ai principigenerali ed ai modelli di organizzazione e gestione. Di seguito i riferimenti:

- **L. 179/2017** che ha modificato l'art. 6 introducendo la lettera d) del comma 2 bis ed i commi 2 tere quater prevedendo:
  - Lett. D, il modello di organizzazione e gestione prevede che nel sistema disciplinare adottato ai sensi del comma 2 lettera e) siano comminate sanzioni nei confronti di chi viola le misure di tuteladel segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate;
  - comma 2 ter, l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2 bis può essere denunciata all'Ispettorato Nazionale del Lavoro, per iprovvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo;
  - comma 2 quater, il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo.Sono altresì nulli il mutamento delle mansioni ai sensi dell'art. 2013 c.c., nonché qualsiasi altramisura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legali all'irrogazione di sanzioni disciplinari o demansionamenti, licenziamenti, trasferimenti o sottoposizione del segnalante ad altra misura organizzativa aventeeffetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure siano fondate su ragioni estranee alla segnalazione stessa.

Infine, ulteriori modifiche della normativa hanno avuto ad oggetto la durata delle misure cautelari, sanzioni, misure interdittive, confisca e pubblicazione della sentenza a carico dell'Ente.

2.2 Esimenti della Responsabilità

Il Decreto prevede una specifica esimente dalla responsabilità amministrativa qualora l'Ente dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto illecito, modellidi organizzazione e gestione, idonei a prevenire la realizzazione degli illeciti penali considerati;

b) ha affidato, ad un organo interno (di seguito "Organismo di Vigilanza") dotato di autonomi poteri d'iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'efficace osservanza del modello, nonché il compito di curarne l'aggiornamento;

c) le persone che hanno commesso il reato hanno agito fraudolentemente eludendo il modello;

d) non vi è stato omesso o insufficiente controllo da parte dell'Organismo di Vigilanza.

Ai sensi dell'articolo 6, comma 2, il Decreto prevede inoltre che i Modelli di organizzazione e gestione debbano rispondere alle seguenti esigenze:

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

2.3 Il confine territoriale di applicazione della responsabilità da reato 231/01 (i reati commessi all'estero)

L'art. 4 del Decreto 231/01 disciplina i reati commessi all'estero, prevedendo che gli Enti avente sede principale sul territorio italiano rispondano anche in relazione a reati presupposto commessi all'estero, nei casi e alle condizioni previsti dagli artt. 7 e 10 c.p., purché nei loro confronti non proceda lo Stato in cui è stato commesso il fatto.

Dunque, l'Ente è perseguibile quando:

- in Italia ha la sede principale, cioè la sede effettiva ove si svolgono attività amministrative e di direzione, ovvero il luogo in cui viene svolta l'attività in modo continuativo (Enti privi di personalità giuridica);
- nei confronti dell'Ente non stia procedendo lo Stato in cui è stato commesso il fatto;
- la richiesta del Ministro di grazia e Giustizia. Qualora la normativa preveda che l'autore del reato sia punito a richiesta del Ministro della Giustizia, si procede contro l'Ente solo se la richiesta sia formulata anche nei confronti di quest'ultimo.

2.4 Le sanzioni applicabili

Le sanzioni amministrative per gli illeciti amministrativi dipendenti da reato sono:

a) sanzioni pecuniarie;

La sanzione pecuniaria è determinata dal giudice attraverso un sistema basato su quote, di valore variabile secondo parametri prestabiliti dal Decreto.

L'importo di una quota va da un minimo di euro 258,00 a un massimo di euro 1.549,00.

Nel determinare l'entità della singola quota il giudice tiene conto delle condizioni economiche e patrimoniali dell'Ente allo scopo di assicurare l'efficacia della sanzione.

In sede di determinazione della sanzione, il giudice stabilisce altresì il numero delle quote applicabili - non inferiore a 100 né superiore a 1.000 -, tenuto conto della gravità del reato, del grado di responsabilità dell'Ente, dell'attività svolta per eliminare le conseguenze del fatto e attenuarne le conseguenze e per prevenire la commissione di altri illeciti

b) sanzioni interdittive;

c) accessorie

- confisca;
- pubblicazione della sentenza.

In particolare, le principali sanzioni interdittive concernono:

1. l'interdizione dall'esercizio delle attività;
2. la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
3. l'esclusione da agevolazioni, finanziamenti, contributi e sussidi, nonché la revoca di quelli eventualmentegià concessi;
4. il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
5. il divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive, tuttavia, non si applicano - o sono revocate se applicate in via cautelare - qualora l'Ente, prima della dichiarazione di apertura del dibattimento di primo grado (ex art. 17 d.lgs. 231/01):

- abbia risarcito il danno o lo abbia riparato;
- abbia eliminato le conseguenze dannose o pericolose del reato o, almeno, si sia efficacemente adoperato in tal senso;
- abbia messo a disposizione dell'autorità giudiziaria, per la confisca, il profitto del reato;
- abbia eliminato le carenze organizzative che hanno determinato il reato, adottando e rendendo operativi modelli organizzativi idonei a prevenire la commissione di nuovi reati della specie di quello verificatosi.

Infine, con L. 9/1/2019 n. 3 (c.d. Spazzacorrotti) sono state introdotte sanzioni interdittive per alcuni reati contro la P.A. e relativo inasprimento del trattamento sanzionatorio. Pertanto, le sanzioni interdittive, in questi specifici casi, avranno una durata compresa tra 4 e 7 anni se reato commesso da apicale, e da 2 a 4 anni da soggetto subordinato. Qualora ricorrano tutti questi comportamenti, di ravvedimento operoso, la sanzione interdittiva è sostituita da quella pecuniaria.

2.5 Le misure cautelari

Il Decreto ha previsto la possibilità di applicare in via cautelare alcuni provvedimenti volti a realizzare una tutela anticipata in caso di condanna dell'Ente.
Per l'applicazione delle misure cautelari è necessario che sussistano gravi indizi di responsabilità per l'Ente e fondati e specifici elementi di concreto pericolo di reiterazione del reato per il quale si procede.
Una volta accertato che sia possibile procedere con le misure cautelari, il giudice deve determinarle tenendo conto della specifica idoneità delle stesse in relazione alla natura e al grado delle esigenze cautelari da soddisfare nel caso concreto; deve poi tenere conto del principio di proporzionalità delle stesse all'entità del fatto e alla sanzione eventualmente applicabile.

Le misure cautelari possono essere rappresentate da provvedimenti interdittivi, dal commissariamento giudiziale, dal sequestro preventivo e dal sequestro conservativo.
Il commissariamento giudiziale presuppone la prosecuzione dell'attività dell'Ente per opera di un commissario. In genere si utilizza tale strumento in luogo della misura interdittiva:

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

Il sequestro preventivo si applica esclusivamente su beni per cui sia consentita la confisca, vale a dire il profitto e il prodotto del reato.
Il sequestro conservativo è volto in via cautelare a preservare le garanzie per il pagamento della sanzione,

delle spese del procedimento o di ogni altro importo dovuto all'Erario e colpisce i beni mobili e immobili dell'Ente, le somme o le cose di cui sia creditore.

3. IL MODELLO ADOTTATO DA System Management

Premesso quanto sopra, System Management S.P.A ha adottato il presente Modello di Organizzazione, Gestione e Controllo ed il Codice Etico, ritenendo che l'insieme di tali documenti, al di là delle prescrizioni di legge, costituisca un ulteriore valido strumento di sensibilizzazione dei propri dipendenti e degli altri soggetti alla stessa legati (collaboratori, consulenti, ecc.).
Tutto ciò affinché i suddetti soggetti seguano, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti in linea con i valori etico-sociali cui s'ispira System Management S.P.A. nel perseguimento del proprio oggetto sociale, e tali comunque da prevenire il rischio di commissione dei reati contemplati dal Decreto.
In attuazione di quanto previsto dal Decreto, l'organo direttivo di System Management S.P.A. ha altresì costituito l'Organismo di Vigilanza, attribuendogli i compiti previsti dal Decreto e stabilendo che tale Organismo può farsi assistere da altri soggetti, tra cui i revisori interni, la funzione risorse umane, consulenti legali (per maggiori dettagli sull'Organismo di Vigilanza si rimanda sotto, all'apposito capitolo del presente Modello).

Il Modello si fonda su un complesso, strutturato ed organico, di procedure e controlli finalizzati al presidio delle attività aziendali maggiormente esposte, anche solo potenzialmente, alla commissione dei reati contemplati dal Decreto, per prevenirne o impedirne la commissione.
In particolare:
a) individua le aree ed i processi fonti di possibili rischi nell'attività aziendale, con particolare riguardo a quelle che comportano un rischio di reato ai sensi del Decreto
b) definisce un sistema organizzativo internodiretto a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai rischi/reati daprevenire tramite:

I. un sistema normativo – composto dal Codice Etico della Società – che fissa le linee di orientamento generali,formalizzate nel tempo, tese a disciplinare in dettaglio le modalità per assumere ed attuare decisioni nei settori "sensibili";
II. un sistema di deleghe e di poteri aziendali che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni;
III. la definizione di strutture organizzative coerenti ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;

c) coordinandosi con l'OdV, individua i processi di gestione e controllo delle risorse finanziarie, idonee a prevenire la commissione dei reati di cui si tratta nelle attività potenzialmente a rischio;
d) attribuisce all'Organismo di Vigilanza specifici compiti di controllo sull'efficacia e sul corretto funzionamento del Modello, sulla coerenza dello stesso con gli obiettivi e sul suo aggiornamento periodico.

Le finalità del Modello, in conformità al Decreto, sono pertanto quelle di:
I) prevenire e ragionevolmente limitare i possibili rischi connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali condotte illecite;
II) determinare, in tutti coloro che operano in nome e per conto di System Management S.P.A., nelle aree di attività a rischio, la consapevolezza di poter incorrere, nel caso di violazioni alle disposizioni riportate nel Modello anche di sanzioni nei confronti di System Management S.P.A.;
III) ribadire che System Management S.P.A. non tollera comportamenti illeciti, di ogni tipo e indipendentemente da qualsiasi finalità, in quanto gli stessi, oltre a trasgredire le leggi vigenti, sono comunque contrari ai principi etico-sociali cui System Management S.P.A. intende attenersi.

Il Modello si prefigge di indurre tutti quei soggetti che siano in posizione apicale, gli Amministratori, i

dipendenti, nonché coloro che operano per System Management S.P.A., quale che sia il rapporto, anche temporaneo che li lega alla stessa, ad acquisire la sensibilità necessaria per percepire la sussistenza dei rischi di commissione di reati nell'esercizio di determinate attività ed insieme comprendere la portata, non solo personale ma anche societaria, delle possibili conseguenze connesse, in termini di sanzioni penali ed amministrative.
A tal fine, System Management S.P.A. si propone, con l'adozione del Modello, di conseguire il pieno e consapevole rispetto dei principi su cui lo stesso si fonda, così da impedirne l'elusione fraudolenta, e, nel contempo, contrastare fortemente tutte quelle condotte che siano contrarie alle disposizioni di legge ed al Codice Etico societario.

3.1 Modifiche ed integrazioni del modello

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità all'articolo 6, comma 1, lettera a) del Decreto), tutte le modifiche ed integrazioni di carattere sostanziale, che si rendano necessarie per sopravvenute esigenze aziendali ovvero per adeguamenti normativi ovvero in accoglimento dei suggerimenti dell'Organismo di Sorveglianza, sono rimesse alla competenza dell'organo direttivo di System Management S.P.A..
È attribuito all'Organismo di Vigilanza il potere di proporre modifiche al Modello o integrazioni di carattere formale nonché quelle modifiche ed integrazioni del Modello consistenti nella:
I) introduzione di nuove procedure e controlli nel caso in cui non sia sufficiente una revisione di quelle esistenti;
II) revisione dei documenti e delle procedure aziendali e societari che formalizzano l'attribuzione delle responsabilità e dei compiti alle posizioni responsabili di strutture organizzative "sensibili" o comunque che svolgono un ruolo di snodo nelle attività a rischio;
III) introduzione di ulteriori controlli delle attività sensibili, con formalizzazione delle iniziative di miglioramento intraprese in apposite procedure;
IV) evidenziazione delle esigenze di integrare regole di carattere generale.

3.2 Obbligo di conoscenza del modello

È obbligo dei dirigenti, dei dipendenti e dei collaboratori di System Management S.P.A. conoscere il Codice Etico e, nelle sue parti essenziali, il presente Modello. (https://sysmanagement.it/it/etica-dimpresa/)

3.3. Analisi dei rischi

Come sopra esposto, con riferimento alle fattispecie di reato presupposto previste dal Decreto e suscettibili di configurare la responsabilità amministrativa della Società, sono state identificate quelle astrattamente applicabili alla realtà dell'Ente.
Successivamente si è proceduto a individuare per ogni categoria di reato le attività e i processi cd. "sensibili". Tutto ciò ha consentito una verifica capillare dei processi aziendali di volta in volta coinvolti e quindi un'individuazione tra essi di quelli suscettibili di essere considerati "aree a rischio".
Per ciascuna area di rischio è stata, poi, eseguita un'analisi volta a mettere in luce:
- le attività a rischio reato;
- i reati ipotizzabili;
- le possibili modalità di compimento dei reati ipotizzabili;
- i soggetti normalmente coinvolti;
- il grado di rischio;
- strumenti di controllo esistenti;
- eventuali piani di miglioramento.

Il risultato di tale analisi ha evidenziato la sensibilità della Società alla commissione dei reati presupposto indicati nella parte speciale.
Il principio adottato per la **valutazione del rischio** segue la formula utilizzata anche nel sistema della sicurezza sul lavoro, con la formula Probabilità (P) per Danno (D) uguale Rischio (R), attribuendo ad ogni percentuale di

Probabilità un valore e ancorando il parametro del Danno al tipo di sanzione applicabile per il reato contestato (pecuniaria, interdittiva o entrambe).
Al fine di ridurre tale valore di rischio, è bene precisare che il Danno – proprio perché parametrato dall'Autorità Giudiziaria competente – non potrà essere modo ridotto con azioni correttive e/o preventive da parte dell'Ente.
Viceversa, con riferimento alla Probabilità, si indicano di seguito le **misure correttive** che l'Ente potrà adottare al fine di ridurre la possibilità di accadimento dell'evento:
- Adozione del Codice Etico e di disciplina
- Adozione di documenti di settore (es. DVR per la sicurezza sul lavoro)
- Adozione policy interne (es. anticorruzione) e appendici (es. fiscali)
- Adozione di un sistema di Deleghe e Procure
- Certificazioni
- Nomina di un DPO, di un sistema MOP.

Un concetto fondamentale nella costruzione di un Modello organizzativo è quello di **rischio accettabile**. Infatti, ai fini dell'applicazione delle norme del Decreto è importante definire una soglia che permetta di porre un limite alla quantità e qualità degli strumenti di prevenzione da introdurre per inibire la commissione del reato.
Infatti, come ribadito dalle Linee Guida di Confindustria di giugno 2021, il rischio è ritenuto accettabile quando i controlli aggiuntivi "costano" più della risorsa da proteggere.
Il rischio è accettabile, nei casi di reati dolosi, allorquando l'efficacia del sistema di prevenzione alla commissione del reato è tale da poter essere aggirata solo fraudolentemente (cd. Elusione fraudolenta del Modello quale esimente) .
Nei reati colposi il rischio accettabile è rappresentato dalla realizzazione di condotte in violazione del Modello organizzativo di prevenzione, nonostante la puntuale osservanza degli obblighi di vigilanza.

La gestione dei rischi interviene anche per il tramite di sistemi di controllo preventivo ed il loro continuo aggiornamento. Si tratta in sostanza di progettare protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione dei reati da prevenire. Tali presidi si concretizzano in tre diversi livelli di verifica:
1) Primo livello di controllo (cd. Controlli in linea) propri dei processi operativi e vengono svolti da risorse interne in un meccanismo di autocontrollo;
2) Secondo livello di controllo svolto da strutture tecniche indipendenti da quelle di primo livello, vedasi per la sicurezza l'attività svolta dal RSPP;
3) Terzo livello di controllo, per aziende strutturate di grandi dimensioni, effettuato dall'internal audit che fornisce valutazioni indipendenti e piani di miglioramento definiti in accordo con il management ma anche sa controlli di enti terzi, quali Collegio Sindacale, Società di Revisione e lo stesso OdV.

4. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA

Da un punto di vista generale, all'Organismo di Vigilanza (di seguito anche "OdV"), spettano essenzialmente due tipi di attività, che tendono ad eliminare e/o ridurre i rischi di commissione dei reati, e precisamente:
a) vigilare l'osservanza da parte dei destinatari del Modello delle prescrizioni in esso contenute (funzione ispettiva e repressiva dei reati);
b) verificare i risultati raggiunti dall'applicazione del Modello in ordine alla prevenzione di reati e valutare la necessità o semplicemente l'opportunità di adeguare il Modello a norme sopravvenute ovvero alle nuove esigenze aziendali (funzione preventiva dei reati).
Per lo svolgimento del proprio operato l'OdV deve mantenere immutati certi requisiti in capo ai suoi componenti:
- connotazione specialistica. Tale indicazione è ripresa altresì nella Relazione di accompagnamento al decreto 231/01;

- autonomia, così come disciplinato dall'art. 6, comma 1, lettera b) d.lgs. 231/01 e indipendenza, secondo la quale l'OdV non potrà mai assumere compiti operativi . L'espressione dell'autonomia dell'OdV interviene anche attraverso il conferimento al medesimo di un budget di spesa, di un riconoscimento economico in capo a ciascun membro per le attività svolte e le responsabilità assunte, nonché la dotazione in capo all'Organismo di un proprio Regolamento;
- professionalità: si riferisce al bagaglio culturale e tecnico del componente, che si trasfonde altresì nel curriculum e nella specifica, inserita all'interno del Modello, che ciascun membro abbia competenze in attività ispettive, consulenziali, oltre a conoscenze tecniche utile all'effettivo potere di controllo . È auspicabile altresì che almeno un membro dell'organismo abbia competenze giuridiche "… e, più in particolare, penalistico".

In estrema sintesi, le attività di cui sopra, sono finalizzate all'effettuazione, da parte dell'Organismo di Vigilanza, di una costante vigilanza in merito al recepimento, all'attuazione e all'adeguatezza del Modello. Qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente spetterà all'Organismodi Vigilanza adottare tutte le iniziative necessarie per correggere tale condizione:
a) sollecitando i responsabili delle singole unità organizzative al rispetto dei modelli di comportamento;
b) indicando direttamente quali correzioni e modifiche debbano essere apportate ai protocolli;
c) segnalando i casi di mancata attuazione del Modello ai responsabili ed agli addetti ai controlli all'interno delle singole funzioni e riportando, per i casi più gravi, direttamente all'organo direttivo.

Qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di adeguamento dello stesso, che peraltro risulta integralmente e correttamente attuato, ma si riveli non idoneo allo scopo di evitare il rischio del verificarsi di taluno dei reati previsti dal Decreto, l'Organismo di Vigilanza dovrà attivarsi affinché vengano apportati, in tempi brevi, i necessari aggiornamenti.
Su di un piano più operativo, le suindicate funzioni si tradurranno nelle seguenti azioni:
a) effettuare interventi periodici, sulla base di un programma annuale approvato dall'organo direttivo, volte all'accertamento di quanto previsto dal Modello ed in particolare vigilare:

- affinché le procedure ed i controlli da esso contemplati siano posti in essere e documentati in maniera conforme;
- affinché i principi etici siano rispettati;
- sull'adeguatezza e sull'efficacia del Modello nella prevenzione dei reati di cui al Decreto;
- segnalare eventuali carenze/inadeguatezze del Modello nella prevenzione dei reati di cui al Decreto e verificare che il Management provveda ad implementare le misure correttive;
- suggerire procedure di verifica adeguate, tenendo comunque sempre presente come rimanga in capo al Management della Società, e agli organi sociali specificatamente deputati, la rispettiva responsabilità di controllo delle attività sociali;
- avviare indagini interne straordinarie laddove si sia evidenziata o sospettata la violazione del Modello ovvero la commissione dei reati;
- verificare periodicamente gli atti societari più significativi ed i contratti di maggior rilievo conclusi dalla società;
- promuovere iniziative per diffondere la conoscenza e l'effettiva comprensione del Modello tra i dipendenti ed i collaboratori predisponendo la documentazione interna (istruzioni, chiarimenti, aggiornamenti) ovvero specifici seminari di formazione;
- coordinarsi con i responsabili delle varie funzioni aziendali per il controllo delle attività nelle aree a rischioe confrontarsi con essi su tutte le problematiche relative all'attuazione del Modello (es. definizione clausole standard per i contratti, organizzazione di corsi per il personale, ecc.).

In particolare, l'Organismo di Vigilanza dovrà coordinarsi con le funzioni competenti presenti in Società per i diversi profili specifici:

- per uno scambio di informazioni al fine di tenere aggiornate le aree a rischio reato. In particolare, le funzioni aziendali dovranno comunicare per iscritto i nuovi rapporti con la Pubblica Amministrazione non già a conoscenza dell'Organismo di Vigilanza; per i diversi aspetti attinenti

all'attuazione del Modello;

- per garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace vengano intraprese tempestivamente;
- per mantenere il Modello aggiornato, adeguandolo alle normative sopravvenute ovvero a mutamenti organizzativi della Società e/o a differenti esigenze aziendali;
- per verificare l'aggiornamento della mappa delle attività a rischio, attraverso il compimento di verifiche periodiche puntuali e mirate su tali attività. A tal fine all'Organismo di Vigilanza devono essere segnalate da parte del management e da parte degli addetti alle attività di controllo, nell'ambito delle singole funzioni, leeventuali situazioni che possono esporre l'Azienda al rischio di reato;
    - raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute sul rispetto del Modello, nonchéaggiornamento della lista delle informazioni che allo stesso devono essere trasmesse;
    - verificare che gli elementi previsti dalle singole Parti Speciali del presente Modello siano comunque adeguate e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto. A tal fine, l'Organismo di Vigilanza deve avere libero accesso, senza la necessità di alcun consenso preventivo, salvi i casi in cui tale consenso preventivo sia reso necessario da leggi e regolamenti, a tutta la documentazione aziendale, nonché la possibilità di acquisire dati ed informazioni rilevanti dai soggetti responsabili.

L'Organismo di Vigilanza deve essere inoltre dotato di un budget adeguato all'espletamento delle attività necessarie al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte ecc.) e deve avere la possibilità di avvalersi di consulenti esterni, coordinandosi ed informando preventivamente le funzioni aziendali interessate.

In caso di Organismo di Vigilanza, in forma collegiale, questo, in relazione agli aspetti concernenti la programmazione delle attività, le modalità di verbalizzazione delle riunioni, la disciplina dei flussi informativi,la nomina dell'eventuale Presidente e Segretario, le modalità di convocazione, emanerà un regolamento a disciplina di tali aspetti, da ratificarsi da parte dell'organo direttivo.

4.1. Reporting dell'Organismo di vigilanza

L'Organismo di Vigilanza, salve le ulteriori variazioni strutturali connesse all'evoluzione del Modello, osserverà due linee di reporting con diverso riferimento temporale:
a) reporting periodico con cadenza almeno annuale al Collegio Sindacale, o altro organo di controllo equipollente, ed all'organo di gestione;
b) reporting continuativo al Collegio Sindacale, o ad altro organo di controllo equipollente, ed all'organo di gestione.

Premesso che la responsabilità del Modello permane in capo all'organo direttivo della Società, l'Organismodi Vigilanza riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.
Più specificatamente, l'Organismo di Vigilanza nei confronti dell'organo direttivo, ha la responsabilità di:
a) comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
b) comunicare periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli.

L'OdV, salvo che sussistano particolari esigenze di riservatezza e confidenzialità per l'espletamento delle proprie funzioni, informa tempestivamente il CdA in merito a circostanze e fatti significativi del proprio ufficio o a eventuali urgenti criticità del Modello emerse nell'ambito dell'attività di vigilanza ovvero riferite dai Responsabili di Area.

L'OdV redige, almeno semestralmente, una relazione scritta per il CdA e, se da questo richiesto, per altri Organi di Controllo. Detta relazione deve contenere, quanto meno, le seguenti informazioni:

a) la sintesi delle attività svolte nell'anno dall'OdV;
b) una descrizione delle eventuali problematiche sorte riguardo alle procedure operative di attuazione delle disposizioni del Modello;
c) una descrizione delle eventuali nuove attività a rischio di reato individuate;
d) il resoconto, nel rispetto della riservatezza, delle segnalazioni ricevute da soggetti interni ed esterni, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione nonché alla violazione delle previsioni del Codice Etico, e l'esito delle conseguenti verifiche effettuate;
e) informativa in merito all'eventuale commissione di reati presupposto;
f) i provvedimenti disciplinari e le sanzioni eventualmente applicate dalla Società, con riferimento alle violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione nonché del Codice Etico;
g) una valutazione complessiva sul funzionamento e l'efficacia del Modello con eventuali proposte di integrazioni, correzioni o modifiche;
h) la segnalazione degli eventuali mutamenti del quadro normativo o significative modificazioni dell'assetto interno della Società o delle modalità di svolgimento delle attività d'impresa che comportano un aggiornamento del Modello;
i) la segnalazione dell'eventuale situazione di conflitto di interesse, anche potenziale;
j) il rendiconto delle spese sostenute.

Tale relazione deve essere correttamente conservata e custodita, al fine anche di evitare l'accesso a soggetti estranei all'OdV e al Board.

4.2 Reporting verso l'Organismo di Vigilanza

La documentazione, anche se proveniente da terzi, riguardante l'attuazione del Modello va inoltrata all'Organismo di Vigilanza con le modalità stabilite nelle procedure di controllo.
A tal fine, System Management S.P.A. si doterà di "canali informativi dedicati" per facilitare l'afflusso di informazioni, segnalazioni e comunicazioni verso l'Organismo di Vigilanza.
I dipendenti e gli Organi societari dovranno segnalare all'Organismo di Vigilanza le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei Reati ovvero notizie in merito a comportamenti non in linea con il Codice Etico ovvero con il Modello. La mancata segnalazione costituirà infrazione disciplinare.
I dipendenti con la qualifica di Dirigente avranno l'obbligo di segnalare all'Organismo di Vigilanza le violazioni del Modello commesse dai Dipendenti che a loro rispondono gerarchicamente, nonché di quelle eventualmente commesse da altri Dirigenti e/o da soggetti apicali.
In particolare, l'obbligo di fornire informazioni all'OdV riguarda tutte le Funzioni aziendali, come specificate nell'Appendice, che potranno comunicare:
- report – periodici - riepilogativi delle attività di controllo svolta;
- schede di sintesi;
- relazioni tecniche;
- valutazioni specifiche;
- qualsiasi altro documento che identifichi anomalie e atipicità riscontrate nell'ambito della propria prestazione lavorativa.

Le informazioni dirette all'OdV potranno riguardare:

- l'emissione e l'aggiornamento dei documenti organizzativi;
- gli avvicendamenti nella responsabilità delle funzioni interessate dalle attività a rischio;
- il sistema delle deleghe e procure aziendali e ogni suo aggiornamento (se previste o individuate);
- gli elementi principali delle operazioni di natura straordinaria avviate e concluse;
- operazioni comunque significative nell'ambito delle aree di rischio, anche alla luce delle indicazioni fornite in Parte speciale;
- tutte le indicazioni utili a valutare l'implementazione del sistema sicurezza (es. ivi compresi l'analisi

degli infortuni e la valutazione dei rischi) e ambiente;

- i rapporti predisposti dai Responsabili di Area e dai Responsabili di Processo, nell'ambito delle loro attività di verifica, dai quali possano emergere fatti, atti, eventi a omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o delle previsioni del Modello e del Codice Etico;
- i procedimenti disciplinari avviati per violazioni del Modello, o per gravi accadimenti commessi dal dipendente ai danni dell'azienda;
- qualsivoglia richiesta di assistenza legale inoltrata dai dirigenti/dipendenti nei confronti dei quali la magistratura procede in ambito 231/01;
- le decisioni relative alla richiesta di erogazione e utilizzo di finanziamenti pubblici;
- qualsivoglia comunicazione da parte della PG o dalle Autorità;
- l'instaurazione di Commissioni di inchiesta interne per contrastare ipotesi di responsabilità 231/01;
- verifica delle commesse acquisite da Enti pubblici o da soggetti che svolgono pubblica utilità;
- le informazioni in merito all'andamento delle attività aziendali come puntualmente definite nell'ambito delle procedure di attuazione dei protocolli previsti nelle Parti Speciali del Modello;
- ogni informazione a qualsiasi titolo utile per l'esercizio delle attività di vigilanza.

Resta inteso che i Responsabili di Area, che inoltrano la comunicazione per la loro specifica area – in caso di giudizio negativo da parte dell'OdV – dovranno astenersi da giudizi o considerazioni al fine di evitare situazioni di incompatibilità, anche potenziale. Le informazioni fornite all'OdV, infatti, mirano a consentirgli di migliorare le proprie attività di pianificazione e i controlli, lasciando alla sua discrezionalità stabilire in quali casi attivarsi.

Si aggiunge che il sistema di reporting sarà efficace in quanto viene garantito il principio di riservatezza delle comunicazioni.
Consulenti e collaboratori in genere saranno tenuti ad effettuare le segnalazioni relative alla commissione, o alla ragionevole convinzione di commissione, dei Reati nei limiti e con le modalità che, ove possibile, dovranno essere previste contrattualmente.

Le segnalazioni devono essere effettuate in forma scritta e, anche nel rispetto della normativa whistleblowing, dovrà essere garantito il rispetto del principio di riservatezza; esse possono avere ad oggetto ogni violazione o sospetto di violazione del Modello e del Codice Etico. Le informative acquisite dall'Organismo diVigilanza saranno trattate, in aderenza al Codice Etico, in modo da garantire:
(a) il rispetto della persona, della dignità umana, del diritto di difesa e della riservatezza e da evitare per i segnalanti qualsiasi forma di ritorsione, penalizzazione o discriminazione, nonché
(b) la tutela dei diritti di enti/società e persone in relazione alle quali siano state effettuate segnalazioni in mala fede e che siano risultate infondate.
Circa la gestione delle segnalazioni anonime, in analogia ai nuovi protocolli whistleblowing, le medesime saranno prese in considerazione solo se relative a fatti circostanziati e/o correlate da specifica documentazione.

L'Organismo di Vigilanza valuterà le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine potrà ascoltare l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere.
Le procedure, aperte d'ufficio o a seguito delle predette segnalazioni, dovranno essere repertoriate secondo ordine cronologico dall'Organismo di Vigilanza in apposito registro dallo stesso conservato e la relativa documentazione dovrà essere raccolta in separati fascicoli aventi numerazione progressiva corrispondente a quella di repertorio.

Sono considerate informazioni da trasmettere obbligatoriamente all'Organismo di Vigilanza quelle riguardanti:
a) le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
b) le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al Decreto;

c) provvedimenti e/o notizie, relative a System Management S.P.A., provenienti da organi di polizia giudiziariao da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
d) le richieste di assistenza legale inoltrate dagli Amministratori, dai Dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dal Decreto;
e) le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
f) le relazioni preparate da responsabili delle varie funzioni aziendali da cui emergano fatti, eventi od omissioni anche solo potenzialmente ricollegabili a fattispecie di reato previste dal Decreto;
g) informazioni sulla evoluzione delle attività attinenti alle aree a rischio individuate dal Modello e/o sulle modifiche della organizzazione aziendale;
h) le operazioni atipiche, le relazioni della società di revisione, le copie dei verbali del Collegio Sindacale, o di altro organo di controllo equipollente, e dell'organo direttivo di System Management S.P.A.;
i) le informazioni, di qualsiasi natura e da chiunque provenienti, concernenti indagini o procedimenti, civili, amministrativi, tributari e/o penali aventi attinenza con i reati previsti dal Decreto e con le specifiche attribuzioni dell'Organismo di Vigilanza.

L'Organismo di Vigilanza potrà proporre all'organo direttivo eventuali modifiche alla casistica suindicata.
All'Organismo di Vigilanza deve essere obbligatoriamente comunicato il sistema delle deleghe di poteri e di firma in vigore in System Management S.P.A. e qualsiasi modifica ad esso riferita.

5. SISTEMA DI WHISTLEBLOWING

Il 29 dicembre 2017 è entrata in vigore la Legge n. 179 - recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" - con l'obiettivo di incentivare la collaborazione dei lavoratori per favorire l'emersione di fenomeni illeciti all'interno di Enti pubblici e privati.
Ne deriva che le imprese dotate di Modello 231 devono disciplinare:
- le modalità per effettuare le segnalazioni whistleblowing;
- le modalità di gestione delle stesse.

Pertanto, l'Ente ha proceduto a predisporre un'appendice *ad hoc* denominata "Procedura per la segnalazione di illeciti e irregolarità (cd. Whistleblowing)" (v. all.).
La società al fine di garantire una gestione responsabile e in linea con le prescrizioni legislative ha implementato un sistema di cd. Whistleblowing volto a tutelare gli autori di segnalazioni dei reati presupposto previsti dal Decreto o di ogni altra irregolarità nell'attuazione del Modello di Organizzazione e Gestione.
Pertanto, ai sensi dell'art. 6 del d.lgs. n. 231/01, comma 2bis, la Società:
- ha istituito canali di segnalazione dedicati che consentano ai soggetti di cui all'art. 5, comma primo lett. a) e b) del d.lgs. n. 231/01, di presentare, a tutela dell'integrità dell'Ente, segnalazioni di condotte illecite rilevanti ai sensi del Decreto, violazioni del presente Modello e ogni altra violazione di leggi, regolamenti politiche, norme o procedure aziendali di cui siano venuti a conoscenza in ragione delle funzioni svolte;
- almeno un canale alternativo di segnalazione idoneo a garantire con modalità informatiche la riservatezza dell'identità del segnalante. Tali modalità possono essere attivate per il tramite dell'attivazione di caselle di posta elettronica;
- vieta ogni atto di ritorsione o discriminatorio, diretto o indiretto, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- tutela, tramite misure ad hoc, il segnalato.

L'Ente ha altresì provveduto all'individuazione del'OdV quale organismo che assumerà qualsivoglia iniziativa, anche investigativa, utile a comprendere il fondamento della segnalazione stessa ed eventualmente, per il tramite delle funzioni aziendali incaricate, erogare procedimenti disciplinari e le relative sanzioni nel rispetto del CCNL di riferimento.

Oggi la nuova disciplina prevede come le denunce debbano essere circostanziate e fondate su elementi precisi e concordanti.

La procedura su indicata prevede altresì la gestione delle segnalazioni anonime purché le medesime siano documentate adeguatamente ovvero circostanziate e intrise di specifici particolari. Ciò anche in attuazione delle disposizioni ANAC .

Resta inteso per la gestione della procedura whistleblowing il rispetto delle indicazioni riportate nel regolamento UE 2016/679 GDPR.

Ogni segnalazione è indirizzata al Destinatario e all'Organismo di Vigilanza che, previa valutazione della sua fondatezza, la trasmette ai soggetti competenti e i canali di segnalazione previsti da [Società] al fine di garantire la tutela del segnalante e del segnalato sono:

i. indirizzo e-mail dedicato segnalazione-odv@sysmanagement.it;

ii. invio di posta raccomandata a/r con l'indicazione "riservata e confidenziale" indirizzata alla c.a. del Presidente dell'Organismo di Vigilanza, ovvero mediante deposito fisico presso la cassetta ad hoc.

Nel caso in cui la segnalazione riguardi l'OdV, la stessa dovrà essere inviata tramite posta raccomandata a/r con l'indicazione "riservata e confidenziale" alla c.a. dell'Amministratore Delegato, presso la sede legale dell'azienda Via G. Porzio, Isola E3 n°4, o all'indirizzo e-mail ad@sysmanagement.it.

Inoltre, ai sensi del comma 2ter del medesimo articolo, ogni eventuale misura discriminatoria o ritorsiva adottata nei confronti del segnalante può essere denunciata dal segnalante o dall'organizzazione sindacale alla quale il medesimo appartiene all'Ispettorato Nazionale del Lavoro.

Infine, ai sensi del comma 2quater, l'eventuale licenziamento o il mutamento di mansioni o qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante sono nulle.

In caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, sarà onere del Datore di Lavoro dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

12.1 Sanzioni connesse alla procedura di Whistleblowing

Codesto Modello, nel rispetto della nuova disciplina, stabilisce il divieto di qualsivoglia atto discriminatorio nei confronti dei Whistleblowers; a ciò si aggiunge l'opportunità di predisporre un sistema disciplinare che preveda la sanzione nei confronti di chi viola le misure a tutela del segnalante nonché di chi effettua, con dolo o colpa grave, segnalazioni infondate, ribadendo quanto riportato all'art. 2, comma 2 quater, d.lgs. 231/01 circa la nullità espressa verso misure ritorsive e discriminatorie (licenziamento, mutamento di lavoro, ecc).

6. FORMAZIONE E INFORMATIVA

6.1. Destinatari del Modello

Il Modello si applica:

- a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società o in una sua unità organizzativa autonoma;
- ai dipendenti della Società, anche se all'estero per lo svolgimento delle attività;
- a tutti quei soggetti che collaborano con la Società in forza di un rapporto di lavoro parasubordinato, quali collaboratori a progetto, prestatori di lavoro temporaneo, interinali, ecc.;
- a coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa,quali legali, consulenti, ecc.;
- a quei soggetti che agiscono nell'interesse della Società in quanto legati alla stessa da rapporti giuridici contrattuali o da accordi di altra natura, quali, ad esempio, *partner* in joint-venture o sociper la realizzazione o l'acquisizione di un progetto di business.

L'Organismo di Vigilanza, sentito il parere dei titolari di rapporti con controparti, stabilisce le eventuali ulteriori categorie di destinatari del Modello, in relazione ai rapporti giuridici ed all'attività svolta dagli stessinei

confronti della Società.

6.2. Comunicazione e formazione

Nell'ambito dell'attività di gestione e formazione del personale operata da System Management S.p.A., si deve prevedere una specifica comunicazione e formazione del personale relativa al Modello, delegando a tale funzione gli uffici di Risorse Umane. Questi, coordinandosi con l'Organismo di Vigilanza competente, devono garantire, attraverso i mezzi ritenuti più opportuni, la sua diffusione e la conoscenza effettiva a tutti i destinatari di cui al punto 7.1.

L'OdV determina le modalità di diffusione ai soggetti destinatari del Modello esterni alla Società. Rientra, altresì, nelle funzioni di amministrazione del personale quella di attuare e formalizzare specifici piani di formazione, con lo scopo di garantire l'effettiva conoscenza del Decreto, del Codice Etico e del Modello daparte di tutte le Direzioni e Funzioni aziendali. L'articolazione dei contenuti e delle sessioni di formazione deve essere differenziata a seconda che il Modello di Organizzazione, Gestione e Controllo *ex* D. Lgs. 231/200si rivolga ai dipendenti nella loro generalità, ai dipendenti che operino in specifiche aree di rischio, ai dirigenti,ai funzionari, all'Organismo di Vigilanza, agli amministratori, ecc., sulla base dell'analisi delle competenze e dei bisogni formativi elaborati dalle Risorse Umane.
La Società garantisce la predisposizione di mezzi e modalità che assicurino sempre la tracciabilità delle iniziative di formazione e la formalizzazione delle presenze dei partecipanti, la possibilità di valutazione del loro livello di apprendimento e del loro gradimento del corso, al fine di sviluppare nuove iniziative di formazione e migliorare quelle attualmente in corso, anche attraverso commenti e suggerimenti su contenuti, materiale, docenti, ecc.
La formazione, che può svolgersi anche a distanza o mediante l'utilizzo di sistemi informatici, e i cui contenuti sono vagliati dall'Organismo di Vigilanza, è operata da esperti nelle discipline dettate dal Decreto.

7 SISTEMA DISCIPLINARE

La predisposizione di un efficace sistema disciplinare (allegato 1) per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per garantire l'effettività del Modello stesso.
Al riguardo, infatti, l'articolo 6, comma 2, lettera e), del Decreto prevede che i modelli di organizzazione e gestione devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".
L'applicazione delle sanzioni disciplinari determinate ai sensi del Decreto prescinde dall'esito di eventuali procedimenti penali, in quanto le regole imposte dal modello sono assunte da System Management S.P.A. in piena autonomia, con lo scopo di regolamentare in senso etico le proprie condotte.
In tale direzione, System Management S.P.A. si avvale di un sistema disciplinare basato sulle seguenti linee d'indirizzo:
a) il sistema disciplinare è diversamente strutturato a seconda dei soggetti destinatari e tiene conto delle limitazioni dettate dalle legislazioni locali;
b) il sistema disciplinare individua esattamente le sanzioni disciplinari da adottarsi nei confronti dei soggetti destinatari, per il caso in cui questi ultimi si rendessero responsabili di violazioni, infrazioni, elusioni,imperfette o parziali applicazioni delle prescrizioni contenute nel Modello, il tutto nel rispetto delle relative disposizioni dei contratti collettivi e delle prescrizioni legislative applicabili;
c)il sistema disciplinare prevede un'apposita procedura di irrogazione delle sanzioni, nel rispetto delle procedure previste dalla legislazione locale;
d) il sistema disciplinare introduce idonee modalità di pubblicazione e di diffusione del relativo codice.

8. MODELLO E CODICE ETICO

Il Codice Etico ed il Modello sono due strumenti complementari ed integrati.

Il Codice Etico (allegato 2) pur essendo parte integrante del Modello organizzativo, è stato adottato in via autonoma per comunicare, a tutti i soggetti cointeressati, i principi di deontologia aziendale cui System Management intende uniformarsi, anche indipendentemente da quanto stabilito dal Decreto.
Il Modello risponde, invece, più specificatamente, alle prescrizioni contenute nel Decreto, ha portata ristretta nell'ambito aziendale e tende a prevenire quelle particolari tipologie di rischi/reati previsti dal Decreto stesso.

9. I GRUPPI DI IMPRESE

Nonostante sia assente a livello ordinistico una disciplina generale del gruppo di imprese (inteso quale raggruppamento di enti dotati di singole e distinte soggettività giuridiche), esistono indici di rilevanza delle società organizzate in forma di gruppo, quali:

- il controllo e il collegamento (art. 2359 c.c.);
- la direzione e il coordinamento (art. 2497 c.c.).

A livello di d.lgs. 231/01 non è prevista una responsabilità diretta del gruppo, bensì una responsabilità degli Enti nel gruppo di impresa, sussistente, in particolare, a carico della capogruppo. Affinché tale responsabilità possa ritenersi sussistente, quest'ultima dovrà essere adeguatamente individuata e motivata in sede giudiziaria.
Perché un'altra società del gruppo possa ritenersi responsabile da reato, occorre che l'illecito commesso nella controllata abbia recato una specifica e concreta utilità (anche non necessariamente di carattere patrimoniale) alla controllante o ad altra società del gruppo.
In sostanza, la holding/controllante potrà ritenersi responsabile per il reato commesso nell'attività della controllata quando:

- l'interesse o vantaggio, immediato e diretto, sia rinvenibile non solo nella controllata ma anche nella controllante;
- vi sia stata una partecipazione a livello di concorso nella commissione del reato da parte di persone collegate in via funzionale alla controllante, per il tramite, ad esempio, di direttive di programmazione fissate dai vertici da ritenersi penalmente illegittime o di coincidenza tra gli apicali della holding con quelli della società controllata.

Premesso che ciascuna società del gruppo è chiamata a un'autonoma valutazione e gestione del rischio oltre che alla predisposizione e attuazione del proprio Modello e alla nomina del proprio OdV (dotato di autonomi poteri di iniziativa e controllo), è contemplato che tali attività possano fare seguito a indicazioni e modalità attuative dettate dalla holding, in funzione dell'assetto organizzativo del gruppo.
Pertanto, non una limitazione o un'eccessiva ingerenza nell'autonomia di ciascuna singola società ma una pianificazione a un più alto livello per il gruppo, al fine di raccordare gli sforzi organizzativi al fine di meglio contrastare fenomeni di criminalità di impresa.
In questo senso, la capogruppo potrà:

- indicare una struttura del codice di comportamento;
- indicare principi comuni del sistema disciplinare;
- indicare principi comuni dei protocolli attuativi;
- prevedere un codice etico di gruppo (che ciascuna società dovrà poi calare nella propria realtà aziendale e calibrare a seconda dell'effettiva esposizione ai rischi reato).

Viceversa, le società controllate – non sempre dotate al loro interno di professionalità specifiche con competenze interdisciplinari – potrebbero avvalersi delle funzioni proprie della capogruppo per un supporto di natura consulenziale, volto ad agevolare l'adozione, l'implementazione e il monitoraggio del proprio Modello, ad esempio richiedendo:

- un supporto per la valutazione di attività/processi a rischio;
- un contributo professionale sui possibili presidi da implementare a fronte delle aree a rischio individuate;
- un aiuto nell'aggiornamento del Modello rispetto alle evoluzioni normative con impatto sulle specifiche

realtà del gruppo rispetto alle indicazioni generali.

La figura dell'Internal Audit – solitamente presente nelle capogruppo – potrebbe essere impiegato per le citate attività di supporto, promuovendo per le controllate un approccio coerente rispetto agli indirizzi della holding, sempre nel rispetto dell'autonomia decisionale di ciascuna organizzazione.

PARTE SPECIALE
(Le singole fattispecie di reato)

1. INTRODUZIONE

Al fine di divulgare la conoscenza degli elementi essenziali dei reati considerati "sensibili" per l'attività di System Management S.P.A., si riporta di seguito una sintetica descrizione dei reati, divisi per tipologia, cui è collegata, secondo le previsioni del Decreto, una responsabilità amministrativa a carico della Società.

A. Reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 D.Lgs.231/2001)

1. Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.);
2. Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro entepubblico o delle Comunità europee (art. 316-ter c.p.);
3. Truffa in danno dello Stato o di altro ente pubblico o delle Comunità Europea (art. 640 comma 2, n.1, c.p.);
4. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
5. Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
6. Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898);
7. concussione (art. 317 c.p.);
8. Corruzione per un atto d'ufficio (art. 318 c.p.);
9. Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.);
10. Circostanze aggravanti (art. 319-bis c.p.);
11. Corruzione in atti giudiziari (art. 319-ter c.p.);
12. Induzione indebita a dare o promettere utilità (art. 319 quater c.p.);
13. Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)
14. Pene per il corruttore (art. 321 c.p.);
15. Istigazione alla corruzione (art. 322 c.p.)
16. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte Penale Internazionale o degli Organi delle Comunità Europee e di funzionari delle Comunità Europee e di stati esteri (art. 322 bis c.p.);
17. Traffico di influenze illecite (art. 346 bis c.p.);
18. Peculato (limitatamente al primo comma) (art. 314 c.p.);
19. Peculato mediante profitto dell'errore altrui (art. 316 c.p.);
20. Abuso d'ufficio (art. 323 c.p.)

B. Delitti informatici e trattamento illecito di dati (art. 24-bis, D.lgs. 231/01)

21. Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);
22. Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
23. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
24. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere unsistema informatico o telematico (art. 615- quinquies c.p.);
25. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art.

617-quater c.p.);

26. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informaticheo telematiche (art. 617-quinquies c.p.);
27. Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
28. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblicoo comunque di pubblica utilità (art. 635-ter c.p.);
29. Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
30. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
31. Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.);
32. Perimetro di sicurezza informatico art 1 D.L.105/2019.

C. Reati societari (art. 25-ter, D.Lgs. 231/01)

33. False comunicazioni sociali (art. 2621 c.c.);
34. Fatti di lieve entità (art. 2621 bis c.c.);
35. False comunicazioni sociali in danno dei soci o dei creditori (art. 2622, comma 1 e 3, c.c.) **modificato in Falsecomunicazioni sociali delle società quotate art. 2622 c.c.**;
36. False comunicazioni sociali delle società quotate (art. 2622 c.c.);
37. Impedito controllo (art. 2625, comma 2, c.c.);
38. Formazione fittizia del capitale (art. 2632 c.c.);
39. Indebita restituzione di conferimenti (art. 2626 c.c.);
40. Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
41. Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
42. Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
43. Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
44. Illecita influenza sull'assemblea (art. 2636 c.c.);
45. Aggiotaggio (art. 2637 c.c.);
46. Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.);
47. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.);
48. Falso in prospetto (art. 2623, comma I e II c.c.);
49. Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624, comma I e II c.c.);
50. Corruzione tra privati (art. 2635, c.c.);
51. Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

D. Delitti contro l'industria ed il commercio (art. 25-bis.1, D.Lgs. 231/01)

52. Turbata libertà dell'industria o del commercio. (art. 513 c.p.);
53. Illecita concorrenza con minaccia o violenza. (art. 513-bis c.p.);
54. Frodi contro le industrie nazionali. (art. 514 c.p.);
55. Frode nell'esercizio del commercio. (art. 515 c.p.);
56. Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
57. Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari. (art. 517-quater c.p.).

E. Delitti contro la personalità individuale (art. 25-quinquies, D.Lgs. 231/01)

58. Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
59. Prostituzione minorile (art. 600-bis c.p.);
60. Pornografia minorile (art. 600-ter c.p.);
61. Detenzione di materiale pornografico (art. 600-quater);

62. Pornografia virtuale (art. 600-quater.1 c.p.);
63. Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.);
64. Tratta di persone (art. 601 c.p.);
65. Acquisto e alienazione di schiavi (art. 602 c.p.);
66. Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.);
67. Adescamento di minorenni (art. 609-undecies c.p.).

F. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies, D.Lgs. 231/01)

68. Omicidio colposo (art. 589 c.p.).
69. Lesioni personali colpose (art. 590 c.p.).

G. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies, D.Lgs. 231/01)

70. Ricettazione (art. 648 c.p.).
71. Riciclaggio (art. 648-bis c.p.).
72. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).
73. Autoriciclaggio (art. 648 ter.1 c.p.).

H. Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 octies.1, D.Lgs. 231/01)

74. Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);
75. Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.);
76. Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.).

I. Delitti in materia di violazioni del diritto d'autore (art. 25-novies, D.Lgs. 231/01)

77. Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis).
78. Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3).
79. Abusiva duplicazione, per trarne profitto, di programmi per elaboratore (art. 171 bis, l. 633/1941).
80. Importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione inlocazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma1).
81. Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2).
82. 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 diopere 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; 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; 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 (art. 171-ter l. 633/1941).

83. Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetto al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941).
84. Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 octies, l. 633/1941).

L. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25-decies, D.Lgs. 231/01).

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

M. Reati Ambientali (art. 25-undecies Dlgs 231/01)

86. Inquinamento ambientale (art. 452-bis c.p.);
87. Disastro ambientale (art. 452-quater c.p.);
88. Delitti colposi contro l'ambiente (art. 452-quinquies c.p.);
89. Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
90. Circostanze aggravanti (art. 452-octies c.p.);
91. Uccisione, distruzione, prelievo o possesso di esemplari di specie animali e vegetali selvatiche protette (art.727-bis, c.p.).
92. Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.).
93. Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n. 150/1992, art. 1, art. 2, art. 3-bis e art. 6);
94. Scarico di acque reflue industriali contenenti sostanze pericolose (varie ipotesi previste dall'art. 137, D.Lgs. 152/2006);
95. Attività di gestione di rifiuti non autorizzata (varie ipotesi previste dall'art. 256, D.Lgs. 152/2006);
96. Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (art. 257, D.Lgs. 152/2006);
97. Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari relativi allatracciabilità dei rifiuti (art. 258, D.Lgs. 152/2006);
98. Traffico illecito di rifiuti (art. 259, D.Lgs. 152/2006);
99. Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.) ;
100. Condotte di falsificazione e detenzione di certificazioni SISTRI falsificate (art. 260- bis, D.Lgs. 152/2006);
101. Emissioni in atmosfera oltre i valori limite o in violazione delle prescrizioni (art. 279, D.Lgs.152/2006);
102. Produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive dell'ozono e dell'ambiente (L. n. 549/1993);
103. Inquinamento provocato dalle navi, doloso e colposo (D. Lgs. n. 202/2007).

N. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25- duodecies)

104. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12- bis, D. Lgs. 25 luglio 1998,n. 286).

O. Reati Tributari (art. 25 quinquiesdecies Decreto 231/2001)

105. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 comma1 D.Lgs. 74/2000);
106. Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000);
107. Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 comma 1 e 2 bis D.Lgs. 74/2000);
108. Occultamento o distruzione di documenti contabili (art. 10 d.lgs. 74/2000);
109. Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000);
110. Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
111. Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000);
112. Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000).

2. ALTRI REATI

Per la natura dell'attività e dell'organizzazione della Società System Management S.P.A., si è scelto di non considerare, come fattispecie rilevanti all'interno del Modello, i reati disciplinati dagli *artt.* ***24– ter*** *(delitti di criminalità organizzata, anche transnazionali)****, 25-bis*** (*falsità in monete, incarta di pubblico credito e in valoridi bollo*), dall'***art 25-quater*** (*delitti con finalità di terrorismo, anche internazionale, o di eversione dell'ordine democratico*), dall'art***. 25-quater 1****. (pratiche di mutilazione degli organi genitali femminili)* ***e 25-sexies*** (*reatia tutela del mercato regolamentato),* non considerando ipotizzabili le relative fattispecie di reati nell'ambito dell'attività svolta dalla Società.
Le attività di analisi relative alle tipologie di reati non prese in considerazione, saranno eventualmente svolte successivamente qualora, a seguito di specifiche valutazioni, esse dovessero essere ritenute pertinenti all'Azienda.
A seguito dell'introduzione del D.lgs. 125 del 21 giugno 2016, che ha modificato l'art. 25 bis del Decreto Legislativo 231 del 2001, si ritiene che i reati previsti dagli **art. 24-ter, 25-bis, 25-quater, 25-quater 1e 25-sexies** siano fattispecie di reato non rilevanti per la natura dell'attività e per l'organizzazione della Società System Management S.P.A. Inoltre per i reati di vendita di sostanze alimentari non genuine come genuine **(previsto dall'art. 25-bis1 D.lgs. 231/2001)**, riduzione o mantenimento in schiavitù o in servitù, prostituzione minorile, pornografia minorile, iniziative turistiche volte allo sfruttamento della prostituzione minorile, trattadi persone, acquisto e alienazione di schiavi **(previsti dall'art. 25-quinquies D.lgs. 231/2001),** si ritiene altresì il rischio di commissione reato non rilevante, in relazione all'attività e all'organizzazione della Società System Management S.P.A.
Da ultimo, si ritengono non applicabili alla società i reati di Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies, D.Lgs. n. 231/2001), aggiunto dalla L. n. 39/2019, i Reati di contrabbando (Art. 25-sexiesdecies, D.Lgs. n. 231/2001) articolo aggiunto dal D.Lgs. n. 75/2020, i Delitti contro il patrimonio culturale (Art. 25-septiesdecies, D.Lgs. n. 231/2001) e il Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies, D.Lgs. n. 231/2001), articoli aggiunti dalla L. n. 22/2022.

3. ATTIVITA' SENSIBILI

Ai sensi di quanto disposto dall'art. 6 comma 1, lett. a) del Decreto, la Società, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera, ha identificato le attività sensibili (suddivise per tipologia di reato), nell'ambito delle quali possano essere potenzialmente commessi i reati previsti dal Decreto 231 del 2001.
Successivamente al fine di prevenire o di mitigare il rischio di commissione di tali reati, la Società ha dunque formulato dei protocolli generali di prevenzione (applicabili a tutte le attività sensibili) e dei protocolli specificidi prevenzione per ciascuna delle attività a rischio identificate.
Di seguito si riportano le schede relative ai reati considerati a rischio commissione.

A. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (artt. 24 e 25 del decreto 231/01)

A.1 Attività sensibili.

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati contro la Pubblica Amministrazione:

- Negoziazione/stipulazione/esecuzione contratti con la P.A. (con particolare riferimento alla gestione del conflitto di interessi)
- Gestione rapporti con la P.A. per ottenimento di autorizzazioni e licenze.
- Selezione ed assunzione del personale e gestione di adempimenti previdenziali e assistenziali relativi al personale dipendente ed ai collaboratori esterni.
- Gestione rapporti con la P.A. per aspetti riguardanti la sicurezza e l'igiene sul lavoro.
- Acquisizione/gestione di contributi/sovvenzioni/ finanziamenti concessi dalla P.A.
- Partecipazione a gare d'appalto per la fornitura di beni/servizi a pagamento.
- Gestione del credito nei confronti della P.A.
- Gestione rapporti con la P.A. per adempimenti fiscali e tributari.
- Gestione di contenziosi giudiziali e stragiudiziali.
- Utilizzo/gestione/ manutenzione di sistemi e/o software per la P.A. o forniti dalla P.A.
- Gestione rapporti con Autorità Pubbliche di Vigilanza e relative verifiche ispettive.
- Gestione dei rapporti con gli Enti di Certificazione.
- Gestione dei flussi finanziari e dei rapporti intercompany

A.2 Aree aziendali a rischio

Sono considerate a rischio tutte le aree aziendali che hanno contatti e rapporti con la Pubblica Amministrazione.

A.3 Il sistema dei controlli

A.3.1 Controlli generali

Oltre al rigoroso rispetto del documento denominato "Codice "Etico, gli standard di controllo generali (ovvero validi per tutte le attività sensibili), prevedono:

- *Segregazione delle attività*: si richiede la costante applicazione del principio separazione delle attività tra chi esegue, chi controlla e chi autorizza.
- *Norme/Altre disposizioni di carattere generale*: è prescritto che le disposizioni aziendali siano sempre idonee a fornire chiari principi generali di riferimento per la regolamentazione dell'attività.
- *Poteri di firma e poteri autorizzativi*: si prevede l'obbligo di fissare costantemente regole formalizzate per l'esercizio di poteri autorizzativi e poteri di firma.
- *Tracciabilità*: si richiede l'esistenza di strumenti che, in relazione ad ogni comunicazione scritta relativa a ciascuna attività, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

In particolare deve essere mantenuta traccia:

- Di ogni comunicazione scritta relativa ai rapporti con la Pubblica Amministrazione in merito a ciascuna attività sensibile
- Di tutti i pagamenti verso e dalla PA e delle motivazioni che li hanno generati.

A.3.2 Controlli specifici

Di seguito si individuano, i controlli specifici previsti per le attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.
Procedure organizzative seguite:

- Tracciamento rapporti con PA
- Raccolta e verifica della documentazione da trasmettere alla PA (anche in caso di ispezione)
- Coerenza delle procure con i soggetti che possono intrattenere rapporti con la PA

- Controllo sull'effettivo impiego di fondi erogati da organismi pubblici
- Definizione di modalità e criteri per la selezione delle procedure alle quali partecipare
- Definizione di modalità e parametri per la determinazione del prezzo e verifica circa la congruità dello stesso rispetto ai riferimenti di mercato, tenuto conto dell'oggetto del contratto e delle quantità
- Definizione delle modalità di approvazione del contratto da parte di adeguati livelli autorizzativi
- Definizione delle modalità e dei criteri per la verifica preventiva/accreditamento/qualifica dei fornitori

Divieto di stipulazione di contratti in autonomia:

- il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente stipulare i contratti che ha negoziato**.**
- tutti gli atti e le comunicazioni formali devono essere gestiti e firmati solo da coloro che sono dotatidi idonei poteri in base alle norme interne.
- deve essere esercitata attività di controllo gerarchico sulla documentazione da presentare alla Pubblica Amministrazione in caso di rapporto commerciale con la stessa.
- mantenimento del monitoraggio sull'avanzamento del progetto realizzativo nei contratti con la Pubblica Amministrazione.

Divieto di accesso a risorse finanziarie in autonomia:

- il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente accedere alle risorse finanziarie e/o autorizzare disposizioni di pagamento.
- Devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative. Deve essere sempre presente un controllo sull'impiego delle risorse, sia di fase che al termine del progetto.
- Le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile.
- L'impiego di risorse finanziarie deve essere motivato dal soggetto richiedente, anche attraverso la mera indicazione della tipologia di spesa alla quale appartiene l'operazione, e autorizzato.
- Nessun pagamento o incasso può essere regolato in contanti, salvo che vi sia espressa autorizzazione da parte della Direzione della Società e comunque per importi che non superino somme gestite attraverso la piccola cassa e nel rispetto della normativa antiriciclaggio.
- La Società deve avvalersi solo di intermediari finanziari e bancari sottoposti a una regolamentazionedi trasparenza e di correttezza conforme alla disciplina dell'Unione Europea.
- Sono preventivamente stabiliti, in funzione della natura della prestazione svolta, limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della Società. Il rimborso delle spese sostenute deve essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute.

Divieto di conferimento di contratti di consulenza o similari in autonomia:

- il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente conferire incarichi di consulenza /prestazioni professionali**.** I consulenti definibili storici devono essere soggetti a rivalutazione periodica, così da verificarne l'economicità, l'affidabilità rispetto all'incarico conferito, la congruenza della prestazione rispetto al mercato di riferimento.

Divieto di conferimento e/o stipula di contratti di intermediazione in autonomia:

- il soggetto che gestisce rapporti con controparti nell'ambito delle fattispecie di attività sensibili non può da solo e liberamente conferire e/o stipulare incarichi/contratti di intermediazione.
- I consulenti esterni sono scelti all'interno di una rosa di professionisti in base ai requisiti di professionalità, indipendenza e competenza. L'incarico è conferito per iscritto con indicazione del compenso pattuito e del contenuto della prestazione.

- I contratti che regolano i rapporti con i consulenti devono prevedere apposite clausole che richiamino gli adempimenti e le responsabilità derivanti dal Decreto e dal rispetto dei principi fondamentali del Modello, che deve essere loro comunicato assieme al Codice di Comportamento.
- Non devono essere corrisposti compensi o parcelle in misura non congrua rispetto alle prestazioni rese alla Società o non conformi all'incarico conferito, alle condizioni o prassi esistenti sul mercato oalle tariffe professionali vigenti per la categoria interessata.
- definizione di modalità e criteri per la corretta attuazione delle politiche commerciali.

Divieto di concessione di utilità in autonomia:

- il soggetto che intrattiene rapporti e/o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente concedere qualsivoglia utilità, omaggio, liberalità.

Divieto di assunzione di personale in autonomia:

- il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente procedere ad assunzioni di personale (rapporti di lavoro);

Criteri di selezione del personale:

- devono essere formalizzati criteri oggettivi di selezione dei candidati. La richiesta di assunzione deve provenire dai responsabili di area mai autonomamente dalla funzione dedicata alle risorse umane.
- Le funzioni che richiedono la selezione e assunzione del personale, devono formalizzare la richiesta attraverso la compilazione di modulistica specifica e nell'ambito di un budget annuale**.** La richiesta deve essere autorizzata dal responsabile competente. I candidati devono essere sottoposti ad un colloquio valutativo che si basa su criteri oggettivi.
- Devono essere preventivamente accertati e valutati i rapporti, diretti o indiretti, tra il candidato e la Pubblica Amministrazione. La valutazione dei rapporti tra dipendenti e Pubblica Amministrazione va ripetuta nel tempo in particolare nel corso di partecipazione di gare pubbliche da parte della società.
- Il sistema di valutazione del personale ed i sistemi incentivanti devono essere improntati a criteri di oggettività, di misurabilità e di congruità in relazione ai vari livelli aziendali, e a seguito di proposta da parte del PM di riferimenti con particolare contezza rispetto al risultato raggiunto dal candidato**;**
- Deve essere individuato, secondo i livelli gerarchici presenti in azienda, il responsabile che autorizza ex ante o ex post (a seconda delle tipologie di trasferte, missioni o viaggi al di fuori dei consueti luoghidi lavoro), le note spese ai soggetti richiedenti.

Sicurezza informatica:

- devono esistere adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nelle leggi vigenti e negli standard internazionali di *Information Security Management System*.

Acquisizione/gestione di contributi/sovvenzioni/ finanziamenti:

- deve esistere segregazione di ruoli e responsabilità nelle fasi di istanza, gestione e rendicontazione in riferimento alla gestione dei finanziamenti, contribuzioni o altre agevolazioni.
- Al responsabile interno per l'attuazione dell'operazione deve essere dato il compito di verificare chele dichiarazioni e la documentazione presentata al fine di ottenere il finanziamento o il contributo siano complete e rappresentino la reale situazione economica, patrimoniale e finanziaria della Società.
- Le risorse finanziarie ottenute come contributo, sovvenzione o finanziamento pubblico devono essere destinate esclusivamente alle iniziative e al conseguimento delle finalità per le quali sono staterichieste e ottenute. Incentivare controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.
- L'impiego di tali risorse è sempre motivato dal soggetto richiedente, che ne attesta la coerenza con le finalità per le quali il finanziamento è stato richiesto e ottenuto.

Obbligo di collaborazione:

- devono esistere direttive che sanciscano l'obbligo alla massima collaborazione e trasparenza nei rapporti con le Autorità di vigilanza.
- Rispetto della procedura relativa ai casi di ispezioni delle Autorità pubbliche in azienda.

Obbligo di segnalazione, archiviazione e conservazione nelle ispezioni:

- in caso di ispezioni, deve esistere uno strumento normativo per l'identificazione di un soggetto responsabile per la gestione dei rapporti con l'Autorità di vigilanza, appositamente delegato dai vertici aziendali. Tale strumento normativo deve disciplinare anche le modalità di archiviazione e conservazione delle informazioni fornite, nonché l'obbligo di segnalazione iniziale e di relazione sulla chiusura delle attività sia verso i vertici aziendali che verso l'ODV.

B. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto)

B.1 Attività sensibili.

Le attività sensibili nell'ambito dei reati previsti dall'art. 24-bis del Decreto, in considerazione dell'attuale operatività di System Management S.P.A., sono le seguenti:

- Gestione dei profili utenti – sin dal momento dell'assegnazione della mansione – e del processo di autenticazione per l'accesso alle informazioni, ai sistemi informativi, alle applicazioni, alla rete.
- Gestione e protezione logica e fisica delle postazioni di lavoro.
- Gestione del processo di assegnazione e dismissione degli asset IT (software e hardware).
- Sicurezza fisica dei centri di elaborazioni dati e locali tecnici IT.
- Gestione e protezione dei dati e delle reti.
- Gestione delle comunicazioni e dell'operatività (scambio di informazioni, log management, patch management, politiche di backup, etc..).
- Gestione degli incidenti e dei problemi di sicurezza informatica.
- Gestione dei controlli crittografici.
- Produzione e/o vendita di programmi informatici, di servizi di installazione e manutenzione di hardware, software, reti.

B.2 Aree aziendali a rischio

Sono considerate a rischio le aree aziendali che si occupano delle attività sopra elencate (Area Sistemi informativi).

B.3 Il sistema dei controlli

B.3.1.Controlli generali

Oltre al rigoroso rispetto del documento denominato "Codice "Etico", i controlli generali relativi alle attivitàin oggetto prevedono:

- *Segregazione delle attività*:

si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza;

- *Norme/Circolari*:

è prescritto che le disposizioni aziendali siano sempre idonee a fornire chiari principi generali di riferimento per la regolamentazione dell'attività, anche per quel che concerne il rispetto della normativa in materia di protezione dei dati personali (Codice della Privacy e disposizioni dell'Autorità Garante per la Privacy).

- *Tracciabilità*:

si richiede l'esistenza di strumenti che assicurino la tracciabilità di ciascuna attività di utilizzo, accesso e gestioni di sistemi informatici.

- *Manuale della Qualità*

si richiede l'osservanza delle specifiche e delle procedure previste dal Manuale della Qualità adottato dalla Società.

B.3.2 Controlli specifici

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standarddi controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Controllo degli accessi

Tale controllo prevede che:

- siano definiti formalmente dei requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
- i codici identificativi (*user-id*) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;
- siano definiti i criteri e le modalità per la creazione delle *password* di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale ed ai sistemi critici o sensibili (ad esempio, lunghezza minima della *password*, regole di complessità, scadenza) che comportino validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche;
- gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete siano oggetto di verifiche periodiche;
- le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti;
- siano definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utenti (con previsione di procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro);
- inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni.
- sia predisposta una matrice autorizzativa – applicazioni/profili/richiedente – allineata con i ruoli organizzativi in essere.

Gestione dei problemi di sicurezza informatica

Tale controllo prevede adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, in particolare che:

- siano implementati controlli di sicurezza – in modo definito e regolamentato – al fine di garantire la riservatezza dei dati interni alla rete e in transito su reti pubbliche;
- siano implementati meccanismi di tracciatura degli eventi di sicurezza sulle reti (ad esempio, accessi anomali per frequenza, modalità, tempi);
- sia regolamentata l'implementazione e la manutenzione delle reti telematiche mediante la definizione diresponsabilità e modalità operative, di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate; inoltre deve essere regolamentata l'esecuzione di attività periodiche di *vulnerability assessment*ed *ethical hacking*;
- siano definiti i criteri e le modalità per le attività di *back up* che prevedano, la frequenza dell'attività, le modalità, il numero di copie, il periodo di conservazione dei dati;
- predisposizione di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi;

procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale siano conformi a disposizioni di legge e contrattuali;

- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi

Tale controllo prevede l'adozione di uno strumento normativo che definisca:

- l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle

applicazioni;
- confidenzialità, autenticità e integrità delle informazioni;
- sicurezza nel processo di sviluppo dei sistemi informativi.

Organizzazione della sicurezza per gli utenti esterni

Tale controllo prevede l'adozione di uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

Sicurezza fisica

Tale controllo prevede l'adozione di misure finalizzare a prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature, in particolare:

- siano definite le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo: *badge*, codici di accesso, *pin* specifici e la tracciabilità degli stessi;
- siano definite le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, la responsabilità, il processo di *reporting* delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;
- presenza di misure per un'adeguata protezione delle apparecchiature incustodite;
- previsione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business;
- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

C. REATI SOCIETARI (art. 25-ter del Decreto)

C.1 Attività sensibili.

La Società ha individuato le attività sensibili di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati societari previsti dall'art. 25-ter del Decreto:

- Tenuta della contabilità, predisposizioni di bilanci, relazioni periodiche, comunicazione di dati societari ad enti pubblici e privati.
- Gestione dei rapporti con organi sociali di controllo, società di revisione ed altri organi societari.
- Tenuta e conservazione, anche con strumenti informatici, di documenti sui quali i soggetti di cui sopra potrebbero esercitare il controllo.
- Predisposizione di documenti ai fini delle delibere assembleari e del Consiglio di Amministrazione.
- Rapporti con Enti Pubblici che svolgono attività regolatorie e di vigilanza.
- Gestione dei finanziamenti pubblici.
- Adempimenti legislativi legati alla gestione di operazioni sul capitale al fine di salvaguardare il patrimonio della società (operazioni su azioni o quote; acconti sui dividendi, fusioni e scissioni, distribuzione degli utili).
- Collaborazione e supporto all'organo amministrativo nello svolgimento di operazioni straordinarie.

C.2 Aree aziendali a rischio

Sono considerate a rischio le aree aziendali che si occupano delle attività sopra elencate (Direzione, Amministrazione e Finanza, Legale Societario e Affari Generali).

C.3 Il sistema dei controlli

C.3.1 Controlli generali

Oltre al rigoroso rispetto del documento denominato "Codice "Etico", i controlli generali relativi alle attivitàin oggetto prevedono:

- *Segregazione delle attività/funzioni/processo*

Si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Normativa aziendale e circolari interne destinate a regolamentare la specifica attività*

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurinola tracciabilità degli elementi informativi e delle relative fonti.

C.3.2 Protocolli specifici di prevenzione

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Per le operazioni di tenuta della contabilità, predisposizioni di bilanci, relazioni periodiche, comunicazionedi dati societari ad enti pubblici e privati, i protocolli prevedono:

- **Norme contabili:** lo standard prescrive che siano portate a conoscenza del personale coinvolto in attività di predisposizione del bilancio, norme che definiscono con chiarezza i principi contabili da adottare per la definizione delle poste del bilancio e le modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente aggiornate dall'ufficio competente alla

luce delle novità della normativa e diffuse aidestinatari sopra indicati.

- **Istruzioni di chiusura contabile:** lo standard dispone la formazione e diffusione di istruzioni che indichinodati e notizie che è necessario fornire agli uffici coinvolti nel processo di redazione del bilancio in relazione alle chiusure annuali ed infrannuali, nonché le relative modalità e la tempistica

- **Flusso informativo e procedure**: lo standard prescrive l'esistenza di una procedura formalizzata che preveda ruoli e responsabilità relativamente al flusso informativo da fornire ai vari uffici coinvolti nel processo di bilancio. Tali procedure dovranno riguardare il corretto comportamento di tutti i dipendenti coinvolti nelle attività di formazione del bilancio o di altri documenti similari, così da garantire: massima collaborazione; completezza e chiarezza delle informazioni fornite; accuratezza dei dati e delle elaborazioni; tempestiva segnalazione di eventuali conflitti di interesse.

- **Tracciabilità:** lo standard stabilisce che il sistema informatico utilizzato per la trasmissione di dati e informazioni debba garantire la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascun Servizio coinvolto nel processo deve garantire la tracciabilità delle informazioni contabili non generate in automatico dal sistema.

- **Lettere di attestazione:** lo standard impone che il soggetto responsabile dell'attività di predisposizione del bilancio acquisisca dai responsabili delle funzioni coinvolte nel processo di bilancio una dichiarazione attestante la veridicità e completezza delle informazioni fornite ai fini della redazione del bilancio civilistico e consolidato.

- **Riunioni tra Società di revisione e organo interno di controllo**: lo standard prescrive che debbano essere effettuate una o più riunioni tra la Società di revisione e l'organo interno di controllo, prima delle riunioni del consiglio di amministrazione e della relativa assemblea indette per l'approvazione del bilancio, che abbiano per oggetto la valutazione di eventuali criticità emerse nello svolgimento delle attività di revisione.

- **Attività di formazione**: lo standard dispone che debbano essere svolte attività di formazione di base, rivolte agli uffici coinvolti nella redazione del bilancio e degli altri documenti connessi, in merito alle principali nozioni ed alle problematiche giuridico-contabili inerenti il bilancio.

- **Conservazione del fascicolo di bilancio**: devono essere formalizzate regole che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio, dall'approvazione del consiglio di amministrazione al deposito e pubblicazione (anche informatica) dello stesso fino alla relativa archiviazione.

- **Norme di gruppo**: devono esistere ed essere diffusi al personale coinvolto in attività di predisposizione dei documenti di cui sopra, strumenti normativi di gruppo che definiscano con chiarezza i principi contabili da adottare per la definizione delle informazioni e dati sulla situazione economica, patrimoniale e finanziariadella Società e delle modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente integrate/aggiornate dalle indicazioni fornite dall'ufficio competente sulla base dellenovità nell'ambito della legislazione primaria e secondaria e diffuse ai destinatari sopra indicati. Devono esistere adeguate procedure amministrative e contabili, a cura del dirigente preposto alla redazione dei documenti contabili societari, finalizzate alla predisposizione del bilancio di esercizio e del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario

Per le operazioni riguardanti la gestione dei rapporti con organi sociali di controllo, società di revisione edaltri organi societari e per quelle di tenuta e conservazione, anche con strumenti informatici, di documenti sucui tali soggetti potrebbero esercitare il controllo, i protocolli prevedono:

- **Direttive:** devono esistere direttive che sanciscano l'obbligo alla massima collaborazione e trasparenza nei rapporti con Collegio Sindacale o altro organo di controllo equipollente, Società di Revisione e altri organisocietari
- **Selezione della società di revisione e sua indipendenza nel mandato**: devono essere regolamentate in una disposizione aziendale le fasi di selezione della società di revisione contabile e devono altresì esistere regole per salvaguardare l'indipendenza della società di revisione nel periodo del mandato
- **Verifica del grado di indipendenza:** deve essere prevista la verifica da parte dell'organo interno di controllo del grado di indipendenza della Società di Revisione alla luce delle regole e criteri fissati per la selezione e valutazione della Società di Revisione
- **Riunioni tra società di revisione ed il collegio sindacale**: devono essere effettuate una o più riunioni, trala Società di Revisione ed il Collegio Sindacale, aventi ad oggetto la valutazione di eventuali criticità emerse nello svolgimento delle attività di revisione
- **Documentazione:** deve esistere l'obbligo di trasmissione alla società di revisione, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione sui quali essa debba esprimere un parere ai sensi di legge o in base ai regolamenti interni
- **Report:** deve essere previsto l'obbligo di report periodici all'organo interno di controllo sulle informazionirichieste dalla e rese alla Società di Revisione, oltre alla previsione di un giudizio sul bilancio (o attestazione similare, sufficientemente chiara ed analitica) da parte della stessa Società di Revisione.
- **Obblighi informativi:** deve essere formalizzare una disposizione aziendale che identifichi ruoli e responsabilità, relativamente agli obblighi informativi della Società (Registro Imprese, ecc.) con riferimento alla stipulazione di patti parasociali. Comunicare all'OdV incarichi conferiti, o che si intende conferire, alla Società di Revisione o a società ad essa collegate, diversi da quelli concernenti la certificazione del bilancio.

Per le operazioni riguardanti la collaborazione e supporto all'organo amministrativo nello svolgimento di operazioni straordinarie, i protocolli prevedono:

- **Documentazione:** deve essere predisposta idonea documentazione relativa alle operazioni in esame.
- **Conservazione del fascicolo di bilancio**: devono esistere regole formalizzate che identifichino ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio, dalla sua approvazione da parte del Consiglio di Amministrazione al deposito e pubblicazione (anche informatica) dellostesso fino alla relativa archiviazione.
- **Procedure**: devono esistere procedure autorizzative per acquisti e vendite di partecipazioni proprie e/o in altre società (esistenza di una procedura per la valutazione, autorizzazione e gestione delle operazioni sulcapitale), nonché una procedura che regolamenti la predisposizione di una relazione per l'organo amministrativo che giustifichi la distribuzione di utili e riserve nel rispetto di quanto previsto dalla legge.
- **Obblighi:** lo standard richiede che debba esistere un obbligo di informativa e di segnalazione agli organi deputati nel caso di iniziative di operazioni sul capitale o di compravendita di azioni o altri strumenti finanziariemessi dalla Società e/o dalle società controllanti. In questo senso, occorrerà osservare 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.

Per le attività di predisposizione di documenti ai fini delle delibere assembleari e del Consiglio di Amministrazione.

- **Gestione del verbale d'assemblea:** devono essere formalizzati in una disposizione aziendale chiara i ruolie le responsabilità, relativamente alla trascrizione, pubblicazione del verbale d'assemblea e conservazione del relativo libro verbali assemblee.

· *Per le attività di gestione di ipotesi di conflitto di interessi*

- Identificazione delle principali fattispecie di interessi degli amministratori.
- Adozione di procedure autorizzative per operazioni esposte a situazioni di conflitto di interesse evidenziate da singoli amministratori.
- Circolarizzare indicazioni sulla necessità di inviare segnalazioni all'OdV in caso di riscontrata presenza di situazioni di conflitto di interesse.

D. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (art. 25-bis.1,)

D.1. Attività sensibili nell'ambito dei delitti contro l'industria e il commercio

Non sussistono ragioni di escludere, in via di principio, la commissione dei reati in oggetto, tranne che per il reato di vendita di sostanze alimentari non genuine come genuine (art.516 c.p.).
Le attività sensibili nell'ambito di delitti contro l'industria ed il commercio, in considerazione dell'attuale operatività di System Management S.P.A., sono le seguenti:

- Gestione delle procedure di acquisto.
- Gestione dei contratti/convenzioni con i fornitori di beni o servizi.
- Gestione delle attività commerciali.

D.2. Aree aziendali a rischio

Sono considerate a rischio tutte le aree aziendali che svolgono le attività sensibili sopra individuate (Direzione, Amministrazione e Finanza, Acquisti e logistica, Legale Societario e Affari Generali).

D.3. Il sistema dei controlli

D.3.1 Controlli generali

Oltre al rigoroso rispetto del documento denominato "Codice "Etico", i controlli generali relativi alle attivitàin oggetto sono descritti di seguito:

- *Segregazione delle attività/funzioni/processo*

Si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Normativa aziendale e circolari interne destinate a regolamentare la specifica attività*

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurinola tracciabilità degli elementi informativi e delle relative fonti.

D.3.2 Controlli specifici

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.

Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici ad oggi pubblicati dalle principali associazioni di categoria.

- **Procedure di selezione dei fornitori di beni /servizi**: con riferimento a tale controllo si applica quanto previsto dai protocolli di prevenzione di cui al paragrafo G della presente Parte Speciale, concernente i reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita
- **Misure idonee a garantire la tracciabilità del processo acquisitivo**, così che emergano in maniera chiara le motivazioni a sostegno di una determinata scelta organizzativa e/o operativa: anche con riferimento a tale tipo di controllo, si applica quanto previsto dai protocolli di prevenzione di cui al paragrafo G della presente Parte Speciale concernente i reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita
- **Prescrizioni comportamentali** che prevedano il divieto di porre in essere comportamenti di qualunque natura che possano fare incorrere la società nella commissione del reato in questione ed in particolare nei confronti di quei soggetti che seguono i processi di approvvigionamento e/o le procedure di gara. Inoltre, viene chiesto a tutti i collaboratori di adottare condotte finalizzate a non intralciare il normale funzionamento delle attività economiche e commerciali delle società concorrenti, rispettando i principi etici tracciati dal Codice Etico aziendale e quanto previsto nel sistema di gestione della qualità.

E. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (art. 25-quinquies)

E.1. Attività sensibili

Non sussistono ragioni di escludere, in via di principio, la commissione dei reati in oggetto, con riferimento agli articoli **600 – quater c.p (detenzione di materiale pornografico) e 600 quater 1. c.p. (pornografia virtuale).** Le attività sensibili nell'ambito di delitti contro la personalità individuale, in considerazione dell'attuale operatività di System Management S.P.A. S.pA., sono le seguenti**:**

- Promozione e/o gestione di iniziative umanitarie e di solidarietà
- Processo di selezione e gestione del personale
- Gestione siti internet e intranet

E.2. Aree aziendali a rischio

La fattispecie di cui all'art. 25 –quinquies non è ricollegabile a specifiche attività d'impresa svolte dalla Società stessa, pertanto potrebbe essere commessa ad ogni livello aziendale.

E.3. Il sistema di controlli

E. 3. 1 Controlli generali

I controlli generali relativi alle attività in oggetto sono descritti di seguito.

- *Segregazione delle attività/funzioni/processi.*

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Normativa aziendale e circolari interne destinate a regolamentare la specifica attività*

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurinola tracciabilità degli elementi informativi e delle relative fonti.

E.3.2 Controlli specifici

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Prescrizioni comportamentali che comprendono:

- Divieto di organizzazione "Attività Sociali" in autonomia, ovvero il soggetto responsabile dell'organizzazione di "Attività Sociali" non può da solo e liberamente conferire incarichi e stipulare contrattidi tale natura;
- divieto di acquisire, utilizzare, diffondere e/o cedere materiale pedopornografico;

Gestione del personale:

- Gestione del processo di selezione del personale;
- Gestione del trattamento normativo ed economico del personale e remunerazione delle prestazioni;
- Gestione del processo di valutazione del personale;
- Attribuzione degli appalti e subappalti (servizi ed opere);
- Procedura di gestione della malattia professionale;
- controlli a cura della che si occupa di risorse umane sul rispetto dalla normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;

- divieto di sottoporre i lavoratori a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Sicurezza dei sistemi:

- esistenza di liste dei siti ai quali è autorizzato l'accesso;
- effettuazione di controlli a campione relativi ai dati ed agli accessi alla rete internet;
- installazione di appositi software volti ad evitare l'accesso a dati non autorizzati o il download di files aventi contenuto riconducibile a quello vietato dalla norma penale.

Controllo accessi:

- Tale standard prevede il controllo degli accessi ai sistemi informativi ed esistenza di automatismi di segnalazione all'amministratore del sistema di operazioni non autorizzate, pertanto, in riferimento a tale controllo si applica quanto previsto dai protocolli di prevenzione di cui al paragrafo B della presente Parte Speciale relativa ai delitti informatici ed al trattamento illecito di dati.

F. OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME, COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (art. 25-septies D.lgs. 231/2001).

Con riferimento all'art. 25septies del Decreto, i reati presupposto possono essere identificati nelle seguenti fattispecie criminose: Omicidio colposo (art. 589 c.p.) e Lesioni colpose gravi o gravissime (art. 590, comma 3, c.p.).

F.1 Attività sensibili

Le aree / attività entro le quali possono verificarsi infortuni o malattie professionali sono desunte dal Documento di Valutazione dei Rischi (nel seguito "DVR"), ove, attraverso attente indagini che interessano sia aspetti strutturali sia aspetti organizzativi, la Società ha individuato i rischi per la sicurezza e la salute dei lavoratori.
Il documento contiene altresì indicate le misure di tutela atte alla loro eliminazione ovvero al loro contenimento.
Per ciascuna delle categorie di rischio presenti nel DVR, trovano collocazione, opportunamente codificati, tutti i pericoli effettivamente applicabili.
Il Documento di Valutazione dei Rischi è costantemente aggiornato, in relazione a nuove ed eventuali esigenze di prevenzione, secondo le procedure previste dal Modello.
Le attività la cui omissione o inefficace attuazione potrebbe integrare una responsabilità colposa della Società, nel caso si verifichi un evento di omicidio colposo o che cagioni lesioni gravi o gravissime, sono riportate di seguito:

- valutazione preliminare di tutti i rischi compresi eventuali rischi interferenziali, individuazione delle misure di tutela e delle risorse necessarie alla eliminazione ovvero al contenimento dei rischi per la salute e sicurezza dei lavoratori;
- definizione delle responsabilità (organigramma della sicurezza);
- sorveglianza sanitaria (gestione delle attività dirette a garantire l'effettuazione della sorveglianza sanitariapreviste per ogni categoria lavorativa);
- formazione del personale generale e specifica;
- affidamento di lavori a soggetti esterni;
- acquisto di attrezzature, macchinari e impianti;
- manutenzione di attrezzature, macchinari e impianti;
- identificazione degli ambienti di lavoro per l'espletamento delle attività lavorative;
- gestione delle emergenze;

- procedure e/o istruzioni di lavoro per l'espletamento delle attività lavorative;
- misure di protezione collettiva e/o individuale atte a contenere o eliminare i rischi;
- coinvolgimento del personale e mantenimento delle misure di protezione implementate nelle segnalazioni di eventuali anomalie.

L'elenco delle suddette attività è periodicamente aggiornato, in relazione a nuove ed eventuali esigenze di prevenzione, secondo le procedure previste dal Modello.

F.2 Aree aziendali a rischio

La fattispecie di cui all'art. 25-septies è ricollegabile a tutte le attività d'impresa, pertanto potrebbe essere commessa ad ogni livello aziendale.

F.3 Il sistema di controlli

F. 3.1 Controlli generali

I controlli generali relativi alle attività in oggetto sono descritti di seguito.

- *Segregazione delle attività/funzioni/processi.*

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Normativa aziendale e circolari interne destinate a regolamentare la specifica attività*

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurinola tracciabilità degli elementi informativi e delle relative fonti.

F.3.2 Controlli specifici

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

F.3.2.1 Principi generali di comportamento

Uno dei presupposti del Modello al fine della prevenzione degli infortuni sui luoghi di lavoro è dato dal rispetto di alcuni principi e nella tenuta di determinati comportamenti, da parte dei lavoratori della Società,nonché dagli eventuali soggetti esterni che si trovino legittimamente presso i locali della Società. In particolare, ciascun lavoratore, ciascun soggetto e più in generale ogni destinatario del Modello che si trovi legittimamente presso la Società dovrà:

- conformemente alla propria formazione ed esperienza, nonché alle istruzioni e ai mezzi forniti ovvero predisposti dal datore di lavoro non adottare comportamenti imprudenti quanto alla salvaguardia della propria salute e della propria sicurezza;
- rispettare la normativa e le procedure aziendali interne al fine della protezione collettiva ed individuale, esercitando in particolare ogni opportuno controllo ed attività idonee a salvaguardare la salute e la sicurezza dei collaboratori esterni e/o di persone estranee, eventualmente presenti sul luogo di lavoro;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze ed i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a disposizione;
- segnalare immediatamente ai livelli opportuni (in ragione delle responsabilità attribuite) le anomalie

dei mezzi e dei dispositivi di cui ai punti precedenti, nonché le altre eventuali condizioni di pericolo di cui si viene a conoscenza;

- adoperarsi direttamente, a fronte di un pericolo rilevato e nei soli casi di urgenza, compatibilmente con le proprie competenze e possibilità;
- sottoporsi ai controlli sanitari previsti;
  sottoporsi agli interventi formativi previsti;
- informare e formare i lavoratori sui rischi propri dell'attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo;
- attribuire specifici compiti e responsabilità in materia di salute e sicurezza sul lavoro, identificando, in maniera formale, i preposti, gli addetti antincendio e primo soccorso, eventuali delegati di funzione;
- contribuire all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro;
- definire gli obiettivi di sicurezza, anche per il tramite del piano di miglioramento, e verificarne il raggiungimento progressivo.

A questi fini è fatto divieto di:

- rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo; compiere di propria iniziativa operazioni o manovre che non sono di propria competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori.

F.4. Controlli generali di prevenzione

Il Documento di Valutazione dei Rischi indica specifiche misure di prevenzione degli infortuni e delle malattie professionali.

Quanto alle misure di prevenzione per le attività a rischio di reato, come sopra identificate, ovvero di quei comportamenti che potrebbero integrare la colpa della Società in relazione a infortuni sul lavoro, il Modello di organizzazione, gestione e controllo è adottato ed attuato al fine di garantire l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione, formazione e addestramento dei lavoratori;
- all'attribuzione di specifici compiti e responsabilità in materia di salute e sicurezza sul lavoro, identificando, in maniera formale, i preposti, gli addetti antincendio e primo soccorso, eventuali delegati di funzione;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezzada parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;
- ove previsto, alle necessarie comunicazioni alle autorità competenti.
  La conformità alle vigenti norme in materia (leggi, norme tecniche e regolamenti, ecc.) è garantita tramite:
- l'identificazione e l'accessibilità alle norme in materia applicabili all'azienda;
- il continuo aggiornamento della normativa applicabile alle attività dell'azienda;
- il controllo periodico della conformità alla normativa applicabile.

Ai fini dell'adozione e dell'attuazione del Modello di organizzazione, gestione e controllo la Società si impegna inoltre a dare attuazione ai protocolli specifici di seguito indicati.

F.5. Controlli specifici di prevenzione

Di seguito sono riportati i protocolli specifici di prevenzione nell'ambito di ciascuna area sensibile a rischio reato identificata e valutata attraverso il *control and risk self-assessment* effettuato dalla Società.

Valutazione dei rischi

La redazione del documento di valutazione dei rischi e del piano delle misure di prevenzione e protezione è un compito non delegabile dal datore di lavoro.

Nomine e definizione delle responsabilità

Per tutte le figure, individuate per la gestione di problematiche inerenti la salute e la sicurezza nei luoghi di lavoro, sono definiti requisiti tecnico-professionali che possono trarre origine anche da specifici disposti normativi. Tali requisiti, che devono essere mantenuti nel tempo, sono in possesso del soggetto preliminarmente all'attribuzione dell'incarico e possono essere conseguiti anche attraverso specifici interventi formativi. Sono, inoltre, applicati provvedimenti disciplinari nel caso di violazioni in materia di sicurezza.

Sorveglianza sanitaria

Preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore è necessario verificarne i requisiti, sia per quanto riguarda gli aspetti tecnici (cfr. l'attività sensibile successiva: Formazione), sia per quanto riguarda gli aspetti sanitari, in base a quanto evidenziato in fase di valutazione dei rischi. Il Medico competente valuta l'adeguatezza ed eventuale aggiornamento del programma di sorveglianza in base alle eventuali sopravvenute esigenze.

DPI

Viene verificata l'idoneità del DPI consegnati sollecitando i destinatari a chiederne il reintegro o la sostituzione in caso di difetti.

Formazione

Tutto il personale riceve opportune informazioni/formazione e nei casi previsti dalla normativa eventuale addestramento circa le corrette modalità di espletamento dei propri incarichi. In particolare, viene garantita una adeguata formazione ai dipendenti in materia di sicurezza sia in occasione dell'assunzione che del trasferimento ad altre mansioni prevedendo sia contenuti formativi di natura generale che specifica sulla base dell'attività svolta dal dipendente; vengono organizzati ed erogati programmi di formazione specifici ai lavoratori, adeguati agli eventuali rischi specifici della mansione cui il lavoratore è in concreto assegnato;

Acquisti

Le attrezzature, i macchinari e gli impianti dovranno essere conformi a quanto previsto dalla normativa vigente (es. marcatura CE, possesso di dichiarazione di conformità rilasciata dall'installatore ecc.). Se del caso,in ragione dei disposti legislativi applicabili, la loro messa in esercizio sarà subordinata a procedure di esame iniziale o di omologazione.

Manutenzione

Tutte le attrezzature, i macchinari e gli impianti che possono avere impatti significativi in materia di Salute e Sicurezza sono assoggettati a protocolli di manutenzione programmata con tempistiche e modalità anche definite dai fabbricanti. Gli eventuali interventi specialistici sono condotti da soggetti in possesso dei requisitidi legge che dovranno produrre le necessarie documentazioni.

Rischi particolari

I luoghi di lavoro sono progettati anche nel rispetto dei principi ergonomici, di comfort e di benessere. Sono sottoposti a regolare manutenzione affinché vengano eliminati, quanto più rapidamente possibile, i difetti che possono pregiudicare la sicurezza e la salute dei lavoratori; sono assicurate adeguate condizioni igieniche.

Eventuali aree a rischio specifico dovranno essere opportunamente segnalate e, se del caso, rese accessibili a soli soggetti adeguatamente formati e protetti.

Emergenze

Sono individuati i percorsi di esodo e si ha cura di mantenerli in efficienza e liberi da ostacoli. Il personale è messo al corrente delle procedure di segnalazione e di gestione delle emergenze. Sono individuati gli addetti agli interventi di emergenza, in un numero sufficiente e sono preventivamente formati secondo i requisiti di legge.

Protezione collettiva ed individuale

In base agli esiti della valutazione dei rischi, devono essere individuati i necessari presidi e dispositivi atti a tutelare il lavoratore. Le misure di protezione di tipo collettivo sono definite nell'ambito della valutazione dei rischi e delle scelte relative, ad esempio, a luoghi di lavoro e attrezzature e macchinari.

Comunicazione e coinvolgimento del personale

La Società adotta idonei mezzi finalizzati a garantire la formazione e l'informazione sulle tematiche della salute e sicurezza sui luoghi di lavoro.

G. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, AUTORICICLAGGIO (art. 25-*octies*)

G.1 Attività sensibili

La Società ha individuato le attività sensibili di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita previsti dall'art. 25-octies del Decreto 231/2001:

- Attività di acquisto e vendita di beni e servizi in Italia e all'estero.
- Gestione dei flussi finanziari, dei fondi aziendali ed impiego di disponibilità liquide attraverso l'utilizzo di ogni strumento di pagamento.
- Gestione sistema dei pagamenti in genere.
- Gestione di operazioni straordinarie, fusioni e acquisizioni.

G.2 Aree aziendali a rischio

Sono considerate a rischio tutte le aree aziendali che svolgono le attività sensibili sopra individuate(Direzione, Amministrazione e Finanza, Legale Societario e Affari Generali).

G.3 Il sistema dei controlli

G.3.1 Controlli generali

I controlli generali relativi alle attività in oggetto sono descritti di seguito e prevedono:

- *Separazione delle responsabilità/funzioni/processo*

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurinola tracciabilità degli elementi informativi e delle relative fonti.

G.3.2 Controlli specifici di prevenzione

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Per le operazioni riguardanti l'attività di acquisto e vendita di beni e servizi i protocolli prevedono:

Definizione di indicatori di anomalia

Siano individuati degli indicatori di anomalia che consentano di rilevare eventuali transazioni a "rischio" o "sospette" con fornitori sulla base del: profilo soggettivo della controparte (es. esistenza di precedenti penali; reputazione opinabile; ammissioni o dichiarazioni da parte della controparte in ordine al proprio coinvolgimento in attività criminose); comportamento della controparte (es. comportamenti ambigui, mancanza di dati occorrenti per la realizzazione delle transazioni o reticenza a fornirli); dislocazione territoriale della controparte (es. transazioni effettuate in paesi offshore); profilo economico-patrimoniale dell'operazione (es. operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica); caratteristiche e finalità dell'operazione (es. uso di prestanome, modifiche delle condizioni contrattuali standard, finalità dell'operazione).

Procedure standardizzate per l'approvvigionamento di beni o servizi che prevedano:

- che l'acquisto di beni e servizi sia disciplinato da contratto scritto, nel quale è chiaramente prestabilito il prezzo del bene o della prestazione o i criteri per determinarlo;
- che i contratti di approvvigionamento di valore significativo siano sempre preventivamente valutati e autorizzati dal Responsabile della funzione che richiede il bene o il servizio;

Per le operazioni riguardanti la gestione dei flussi finanziari, dei fondi aziendali ed impiego di disponibilità liquide attraverso l'utilizzo di ogni strumento di pagamento e gestione sistema dei pagamenti in genere, i protocolli prevedono:

Procedure standardizzate per l'utilizzo dei mezzi finanziari che in particolare dispongano:

- l'utilizzo, per la gestione dei flussi in entrata e in uscita, esclusivamente di canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione europea
- la tracciabilità di tutti gli incassi e i pagamenti della Società nonché in generale di tutti i flussi di denaro della stessa;
- la previsione di limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative;
- la registrazione e documentazione di tutte le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie in conformità ai principi di correttezza professionale e contabile con indicazione anche di una causale espressa;
- l'impiego di risorse finanziarie motivato dal soggetto richiedente, anche attraverso la mera indicazione della tipologia di spesa alla quale appartiene l'operazione;
- il divieto di regolare tutti i pagamenti e gli incassi in contanti, salvo che via espressa autorizzazione da parte della Direzione della Società e comunque per importi che non superino somme gestite attraverso la piccola cassa;

- la previsione di limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della Società. Il rimborso delle spese sostenute deve essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute.

Per le operazioni riguardanti la gestione delle operazioni straordinarie, fusioni e acquisizioni, i protocolli prevedono che:

- Formalizzazione di procedure operative relative al tipo di operazione/processo;
- Verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari.

H. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (art. 25-*octies.1*)

H.1 Attività sensibili

La Società ha individuato le attività sensibili di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati relativi agli strumenti di pagamento diversi dai contanti previsti dall'art. 25-octies.1 del Decreto 231/2001:

- Gestione dei flussi finanziari, dei fondi aziendali ed impiego di disponibilità liquide attraverso l'utilizzo di ogni strumento di pagamento.
- Gestione degli strumenti informatici aziendali con particolare riferimento ai conti correnti on-line
- Gestione e protezione dei dati e delle reti.

H.2 Aree aziendali a rischio

Sono considerate a rischio tutte le aree aziendali che svolgono le attività sensibili sopra individuate (Direzione, Amministrazione e Finanza, IT).

H.3 Il sistema dei controlli

H. 3.1.Controlli generali

I controlli generali relativi alle attività in oggetto sono descritti di seguito e prevedono:

- *Separazione delle responsabilità/funzioni/processo*

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

H. 3.2 Controlli specifici di prevenzione

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Per le operazioni riguardanti la gestione dei flussi finanziari si richiede:

- La verifica della coincidenza tra destinata-ri/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- controllo formale e sostanziale dei flussi finanziari aziendali;

- controllo del flusso di cassa;
- controllo sulle modalità operative di apertura e chiusura dei conti correnti presso banche e istituzioni finanziarie;
- controllo periodico sulla riconciliazione dei conti correnti.

Per le operazioni riguardanti la gestione degli strumenti informatici aziendali si prevede:

- procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche;
- procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro;
- aggiornamento regolare dei sistemi informativi in uso;
- modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto.

Per le operazioni riguardanti la gestione degli strumenti informatici connessi ai conti correnti aziendali:

- utilizzo degli strumenti informatici di pagamento da parte dei soli soggetti autorizzati;
- attività di reporting sulle anomalie bancarie eventualmente riscontrate;
- gestione dei token aziendali o dei codici di accesso bancari a seguito di approvazione da parte di adeguati livelli autorizzativi;
- modifica periodica dei codici di accesso bancari quando suggerito dall'ente creditizio.

H.3.2.1 Principi generali di comportamento

Uno dei presupposti del Modello al fine della prevenzione degli infortuni sui luoghi di lavoro è dato dal rispetto di alcuni principi e nella tenuta di determinati comportamenti, da parte dei lavoratori della Società,nonché dagli eventuali soggetti esterni che si trovino legittimamente presso i locali della Società. In particolare, ciascun lavoratore, ciascun soggetto e più in generale ogni destinatario del Modello che si trovi legittimamente presso la Società dovrà:

- tenere un comportamento corretto, trasparente e collaborativo e osservare quanto stabilito dalle norme di legge e dalle procedure aziendali interne, con riferimento a tutte le attività finalizzate alla gestione delle attività amministrative, alla gestione delle movimentazioni finanziarie;
- assicurare adeguata formalizzazione e tracciabilità delle operazioni di natura finanziaria, che devono essere autorizzate, ricostruibili ex post e adeguatamente motivate, oltre che rispondenti alle effettive esigenze della Società;
- effettuare, per quanto di competenza, un costante monitoraggio dei flussi finanziari aziendali, sia in entrata che in uscita;
- accedere ai sistemi informatici solo previa identificazione da parte dell'utente, tramite credenziali assegnate al singolo soggetto dalla Società;
- adottare misure di protezione del sistema volte a evitare l'accesso allo stesso da parte di terzi in caso di allontanamento dalla postazione;
- utilizzare la connessione a internet solo per gli scopi e il tempo necessario allo svolgimento delle attività che richiedono il collegamento;
- trasmettere file o documenti di proprietà della Società, esclusivamente per finalità strettamente attinenti allo svolgimento dell'attività per cui la trasmissione si è resa necessaria.

È altresì fatto divieto di:

- utilizzare strumenti anonimi per il com-pimento di operazioni di trasferimento di importi rilevanti;
- violare le misure di protezione applicate ai sistemi informatici aziendali;
- installare software non autorizzati dal Responsabile per la sicurezza informa-tica, anche se attinenti all'attività della Società.

I. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE (art. 25-*novies*)

I.1 Attività sensibili nell'ambito dei delitti in materia di violazione del diritto d'autore.
Non sussistono ragioni di escludere, in via di principio, la commissione dei reati in oggetto, con riferimento al *reato di abusiva duplicazione o detenzione di programmi per elaboratori o di illecito utilizzo di banche dati(Art. 171-bis L. 633/1941) ed il reato di cui all'art. 171 comma 1, lett. a-bis, L. 633/1941, di messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere e senza averne diritto di un'opera dell'ingegno protetta.* La Società ha individuato le attività sensibili, di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati in materia diviolazione del diritto d'autore previsti dall'art. 25-novies del Decreto:

- Gestione licenze d'uso prodotti software
- Gestione sito internet aziendale.

I.2 Aree Aziendali a rischio
È considerata a rischio in ragione delle attività sensibili sopra individuate l'area aziendale Sistemi Informativi.

I.3 Il sistema dei controlli
I.3.1 Controlli generali
Oltre al rigoroso rispetto del documento denominato "Codice "Etico" i controlli generali relativi alle attivitàin oggetto prevedono:

- *Segregazione delle attività/funzioni/processi.*

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- *Normativa aziendale e circolari interne destinate a regolamentare la specifica attività*

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

- *Sistema deleghe, poteri di firma e poteri autorizzativi*

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

- *Tracciabilità*

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurinola tracciabilità degli elementi informativi e delle relative fonti.

I.3.2 Controlli specifici di prevenzione
Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, alle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Per le operazioni riguardanti la gestione licenze d'uso prodotti software, i protocolli prevedono:

- Processi di acquisizione delle licenze dei software formalizzati in una procedura operativa interna della Società;
- criteri e modalità per il controllo dell'uso di software formalmente autorizzato e certificato;
- verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o non licenziati e/o potenzialmente nocivi;
- verifiche periodiche sulla regolarità delle licenze dei prodotti e rinnovi delle stesse ove necessario;

- definizione di una policy aziendale la quale preveda espressamente:
  - il divieto di procedere ad installazione di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano la licenza d'uso;
  - il divieto di procedere ad installazione di prodotti software sul personal computer in uso in violazione delleprocedure aziendali in materia;
  - il divieto di utilizzare software/banca dati in assenza di valida licenza, anche nel caso in cui la stessa sia solamente scaduta;
  - l'introduzione, nel caso la presente attività sia affidata in outsourcing, nei contratti che regolano i rapporticon i fornitori del servizio, di apposite clausole che impongono la conformità dei software forniti a leggi e normative ed in particolare alle disposizioni di cui alla Legge 633/1941 e che prevedano la manleva per la Società in caso di violazioni commesse dai fornitori del servizio stessi.

Per le operazioni riguardanti la gestione del sito internet aziendale, i protocolli prevedono:

- Definizione di una policy aziendale per gli utenti, che disponga:
  - le regole per il corretto utilizzo di internet;
  - Il divieto per tutti i dipendenti di diffondere immagini, documenti o altro materiale tutelati dalla normativa
  - in materia di diritto d'autore;
  - meccanismi di monitoraggio del traffico e di tracciatura degli eventi di sicurezza sulle reti (ad es. accessianomali per frequenza, modalità, temporalità);
  - definizione dei requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso
  - remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
  - istituzione e aggiornamento di una *black list* di siti da cui può essere effettuato il *download* di chiavi dilicenza e codici sorgente;
  - meccanismi per la tracciabilità sulle applicazioni delle modifiche ai dati ed ai sistemi compiute dagli utenti.

L. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (art. 25-novies del Decreto)

L.1 Attività Sensibili.

La Società ha individuato le attività sensibili, di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati in materia di violazione del diritto d'autore previsti dall'art. 25-novies del Decreto:

- Gestione rapporti con soggetti aziendali coinvolti in procedimenti giudiziari.
- Gestione rapporti con Autorità Giudiziaria (gestione del contenzioso giudiziale e stragiudiziale di cui sia parte la Società).

L.2 Aree aziendali a rischio

La fattispecie di cui all'art. 25–*novies* risulta essere ricollegabile a tutte le aree e funzioni che sostengono la gestione delle controversie giudiziarie avanti le Autorità (Area Legale Societario e Affari generali)

L.3 Il sistema dei controlli

L.3.1 Controlli generali

I controlli generali prevedono il rigoroso rispetto del codice etico aziendale il quale dispone, fra le altre cose, che i rapporti con l'Autorità Giudiziaria relativi a questioni riguardanti la società, sono improntati al rispetto della veridicità delle informazioni rese nelle testimonianze.

L.3.2 Controlli specifici di prevenzione

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate.
Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.
I protocolli specifici prevedono:

- divieto di attuare comportamenti che possano rientrare nelle fattispecie di reato richiamate dall'articolo 25-*novies* d.lgs. 231/2001.
- l'obbligo di prestare una fattiva collaborazione e rendere dichiarazioni veritiere ed esaustivamente
- rappresentative dei fatti nei rapporti con l'Autorità Giudiziaria e della P.G. delegata alle attività di acquisizione documentale e delle sommarie informazioni;
- l'obbligo per i Destinatari (indagato/imputato, persona informata sui fatti/testimone o teste assistito/imputato in un procedimento penale connesso) chiamati a rendere dichiarazioni innanzi all'AutoritàGiudiziaria in merito all'attività lavorativa prestata, di esprimere liberamente la propria rappresentazione dei fatti e ad esercitare la facoltà di non rispondere accordata dalla legge;
- l'obbligo altresì di mantenere il massimo riserbo relativamente alle dichiarazioni rilasciate ed al loro oggetto, ove le medesime siano coperteda segreto investigativo;
- l'obbligo per tutto il personale di avvisare il Responsabile dell'Area Affari Societari di ogni atto di citazionea testimoniare e di ogni procedimento penale che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente.

Presidi di controllo e flussi informativi verso l'Organismo di Vigilanza

- Controlli da parte dell'Organismo di Vigilanza diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere ed a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale;
- Flussi informativi verso l'Organismo di Vigilanza in caso di modifiche organizzative interne, in particolare sulla Governance e sui poteri decisori e autorizzatori rispetto ai processi aziendali:
- Flussi informativi verso l'Organismo di Vigilanza relativi ad ogni atto di citazione a testimoniare e di ogni procedimento penale che veda coinvolto, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata ocomunque ad essa attinente il personale della società;
- Flussi informativi verso l'Organismo di Vigilanza di aggiornaemento circa lo stato dei procedimenti in corso, che coinvolgano la Società ma anche i propri dipendenti e collaboratori per attività connesse alla Società stessa;
- Flussi informativi verso l'Organismo di Vigilanza in merito alle richieste di assistenza legale inoltrate alla Società dai dipendenti in caso di avvio di un procedimento penale a carico degli stessi.

M. REATI AMBIENTALI (art. 25–undecies del Decreto)

M.1 Attività Sensibili.

La Società ha individuato le attività sensibili, di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati in materia di violazione del diritto d'autore previsti dall'art. 25-*undecies* del Decreto:

- Smaltimento di toner esausti e materiale elettronico
- Violazione della normativa vigente (locale e nazionale) sulla raccolta differenziata in relazione ai rifiuti prodotti in ambienti ad uso ufficio

M.2. Aree aziendali a rischio

La fattispecie di cui all'art. 25–*undecies* risulta non essere ricollegabile a specifiche attività d'impresa svolte dalla Società stessa, pertanto potrebbe essere commesso ad ogni livello aziendale.

M.3 Il sistema dei controlli

M.3.1 Controlli Generali

I rifiuti prodotti in un ambiente ad uso ufficio sono classificabili come urbani e assimilati, pertanto vi è l'obbligo, in base alla normativa vigente a livello nazionale (D.lgs. 152/06) e locale (circolari specifiche Regionali) di

effettuare la raccolta differenziata di alcune tipologie di materiali che variano da Comune a Comune. Pertanto:

- Tutti i Soggetti, ciascuno nella misura e con le modalità richieste dalle proprie funzioni (ed in particolare quelle riconducibili al processo di approvvigionamento), sono stati informati dell'obbligo di attenersi alle disposizioni vigenti in ordine alle modalità di detta raccolta, in particolare per questi materiali principali:
  - Carta/CartoneVetro
  - Lattine PlasticaToner
  - Neon e Componenti ElettriciPile Esauste
  - Farmaci scaduti

M.3.2 Controlli specifici di prevenzione

I protocolli specifici di prevenzione prevedono che:

- le funzioni aziendali che si occupano dei processi di approvvigionamento garantiscono l'attivazione e la stipula di apposite convenzioni con enti esterni autorizzati alla raccolta (es. AMSA per le cartucce esauste / contenitori toner).
- Si debba monitorare e valutare periodicamente gli impatti ambientali generati nello svolgimento delle proprie attività, approfondendone i livelli di rischio ed individuando le opportune misure di prevenzione e controllo;
- informare, formare e sensibilizzare il personale affinché sia attuata una corretta gestione delle problematiche ambientali, in applicazione delle procedure e secondo comportamenti coerenti con la Politica ambientale;
- utilizzare le migliori tecnologie disponibili ed economicamente attuabili per sostenere adeguatamente gli obiettivi ambientali;
- analizzare e valutare preventivamente gli effetti ambientali originati da nuove attività o servizi;
- svolgere le proprie attività in maniera responsabile al fine di prevenire, controllare e ridurre eventuali impatti sull'ambiente;
- prevenire gli inquinamenti del suolo e comunque ridurre le fonti di inquinamento nella propria sede e in qualsiasi altro luogo venga svolta l'attività, favorendo la riduzione dei rifiuti derivanti dal proprio lavoro.

N. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE: (art. 25-duodecies)

N.1 Attività sensibili

Non sussistono ragioni di escludere, in via di principio, la commissione del reato in oggetto, la Società ha individuato pertanto le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbe essere commesso il delitto previsto dall'art. 25-*duodecies* del D.lgs. 231/01:

- Attività di selezione ed assunzione del personale (anche non dipendente)
- Gestione fornitori di servizi di pulizie e del personale interinale

N.2 Aree aziendali a rischio

Le aree di rischio aziendale individuate sono quelle che si occupano della selezione e gestione del personale (anche non dipendente), della selezione e gestione dei fornitori operativi, dei fornitori di servizi di pulizie e del personale interinale.

N.3 Il sistema dei controlli

N.3.1 Controlli generali

Allo scopo di prevenire la commissione del reato da ultimo introdotti, si ritiene che possa essere individuata quale efficace e sufficiente misura di prevenzione generale, l'osservanza dei principi e delle disposizioni adottate dal Codice Etico.

N.3.2. Controlli specifici di prevenzione.

I controlli specifici prevedono la redazione di procedure aziendali che dispongano:

- di verificare al momento dell'assunzione e durante lo svolgimento di tutto il rapporto lavorativo che eventuali lavoratori provenienti da paesi terzi siano in regola con il permesso di soggiorno e, in caso di scadenza dello stesso, abbiano provveduto a rinnovarlo;
- di assicurarsi, nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, che tali soggetti si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
- di assicurarsi con apposite clausole contrattuali che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
- di non fare ricorso, in alcun modo, al lavoro minorile o non collaborare con società che ne facciano uso.

O. REATI TRIBUTARI (art. 25 quinquiesdecies D.231/2001)

O.1 Attività sensibili

La società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati tributari:

- Acquisto di beni e servizi;
- Gestione di flussi monetari e finanziari;
- Gestione dei bonus e dei benefit;
- Emissione di documentazione afferente la contabilità;
- Ricevimento di documentazione afferente la contabilità;
- Predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria;
- Pagamento di imposte.

O.2 Aree a rischio.

Principali soggetti, funzioni e unità organizzative coinvolte: Direzione, Risorse umane, Commerciale, Amministrazione finanza e controllo, Acquisti e logistica, Legale societario e tutti coloro che, a qualsiasi titolo, sono coinvolti nei processi sensibili sopra menzionati.
Tutti i reati contemplati dall'art. 25 quinquiesdecies e di cui al d.lgs.74/2000 risultano potenzialmente commettibili all'interno della Società.

O.3 Il sistema dei controlli

O.3.1 Controlli generali

Oltre al rigoroso rispetto del documento "Codice Etico", gli standard di controllo generale prevedono:

- *Segregazione delle attività*

Costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza

- *Norme/circolari*

Le disposizioni aziendali devono essere sempre idonee a fornire chiariprincipi generali di riferimento per la regolamentazione delle attività

- *Poteri di firma e poteri autorizzativi*

Obbligo di fissare costantemente regole formalizzate per l'esercizio di poteri autorizzativi e poteri di firma

- *Tracciabilità*

Esistenza di strumenti che, in relazione ad ogni comunicazione scritta relativa a ciascuna attività, assicurino la tracciabilità degli elementi informativi e dellerelative fonti.
In linea generale, il sistema di organizzazione per la gestione della materia in oggetto deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, e di segregazione delle funzioni e dei ruoli, in modo chenessun soggetto possa gestire da solo un intero processo, in particolare per quanto attiene l'attribuzione di

responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

Più in particolare con riferimento alle indicate aree sensibili è necessario seguire le seguenti regole di condotta:

- Ai componenti degli organi sociali e ai dipendenti, che per conto della società intrattengonorapporti con l'Agenzia delle Entrate e le Autorità fiscali, deve essere attribuito formale potere in tal senso. I soggetti muniti di poteri verso l'esterno devono agire nei limiti dei poteri ad essi conferiti. I soggetti privi di poteri verso l'esterno devono richiedere l'intervento dei soggetti muniti di idonei poteri.
- Qualunque criticità o conflitto di interesse che dovesse insorgere nell'ambito del rapporto con le autorità fiscali deve essere comunicato per iscritto anche all'OdV.
- I titolari di funzioni e mansioni relative a fisco ed imposte nelle dichiarazioni relative ad esse e nella loro predisposizione, non devono introdurre elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti.

A tale riguardo:

1) devono controllare che le fatture e i documenti contabili si riferiscano a prestazioni effettivamente svolte da parte dell'emittente delle fatture/documenti ed effettivamente ricevute dalla società;

2) non devono registrare nelle scritture contabili obbligatorie, né detenere a fini di prova neiconfronti dell'amministrazione finanziaria fatture o altri documenti per operazioni inesistenti;

3) devono verificare la regolare applicazione dell'imposta sul valore aggiunto, devono astenersi dal compiere operazioni simulate oggettivamente o soggettivamente nonché avvalersi di documenti falsi o di altri mezzi fraudolenti idonei a ostacolare l'accertamento e a indurre in errore l'amministrazione finanziaria.
I medesimi soggetti devono astenersi dall'indicare in dichiarazioni relative a imposte sui redditi o sul valore aggiunto:
   - elementi attivi per un ammontare inferiore a quello effettivoo;
   - elementi passivi fittizi;
   - crediti e ritenute fittizi.

4) devono astenersi dall'emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.

5) devono astenersi dall'occultare o distruggere in tutto o in parte le scritture contabili, o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, con il fine di evadere le imposte sui redditi o sul valore aggiunti, ovvero di consentire l'evasione a terzi.

6) devono astenersi dall'alienare simulatamente o dal compiere altri atti fraudolenti sui proprio su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria, con il fine di sottrarsi al pagamento delleimposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativia dette imposte.

7) devono altresì astenersi dall'indicare nella documentazione presentata elementi attivi inferiori a quelli effettivi o elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila, con il fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.

Approvazione da parte del responsabile apicale della gestione contabile e fiscale
Le dichiarazioni e comunicazioni in materia di imposte sui redditi o sul valore aggiunto non devono essere presentate senza la preventiva approvazione e benestare del Chief Financial Officer.

Tracciabilità
La società deve seguire regole che garantiscano il rispetto della normativa in materia nonché la tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'OdV tutta la documentazione di supporto.
La Società monitora le tempistiche da rispettare per le comunicazioni, denunce e adempimenti nei confronti dell'Amministrazione finanziaria.
Si verificano, inoltre, le attività propedeutiche all'elaborazione delle dichiarazioni fiscali, che includono

l'effettuazione di verifiche complementari sugli elementi destinati a confluire nelle stesse.

Ricorso a servizi di terzi
Nel caso di cui la predisposizione delle dichiarazioni e comunicazioni in materia di imposte sui redditi o sul valore aggiunto fosse affidata a terzi esterni alla società, i terzi stessi dovranno essere vincolati contrattualmente a rispettare gli obblighi e i divieti di cui ai punti che precedono.

In particolare, in detti contratti deve essere contenuta apposita dichiarazione delle controparti:

a) di essere a conoscenza della normativa di cui al d.lgs.231/2001 e delle sue implicazioni per la società;
b) di impegnarsi a rispettare detta normativa e farla rispettare dai propri dipendenti e collaboratori;
c) di non essere mai stati condannati (o aver richiesto il patteggiamento) e di non essere al momento imputati o indagati in procedimenti penali relativi a reati presupposto; nel caso di esistenza di condanna o di procedimento in corso, e sempre che l'accordo sia ritenuto indispensabile e da preferirsi a un contratto con altri soggetti, dovranno essere adottate particolari cautele;
d) di impegno a rispettare il Modello (ed in particolare le prescrizioni della presente Parte Speciale) edil Codice Etico della società, ovvero, nel caso di enti, di aver adottato un proprio analogo Modello e un Codice Etico che regolamentano la prevenzione dei reati contemplati nel Modello e nel Codice Etico della società;
e) di impegnarsi in ogni caso ad astenersi dal compiere attività che possano configurare alcuno dei reati presupposto o che comunque si pongano in contrasto con la normativa e/o con il Modello;
f) di adeguare il servizio a eventuali richieste della società fondate sulla necessità di ottemperare alla prevenzione dei reati presupposto di cui trattasi.

Inoltre, nei contratti con i consulenti e con i prestatori di servizi deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte dei prestatori delle norme di cui al d.lgs. 231/2001 (quali ad es. clausole risolutive espresse, penali).

O.3.2. Controlli specifici di prevenzione.

I controlli specifici prevedono la redazione di procedure aziendali che dispongano:

Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi ai Processi Sensibili di cui trattasi devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente eventuali situazioni di irregolarità o anomalie.

Al fine di mitigare il rischio di commissione dei reati presupposto previsti dall'art. 25 quinquiesdecies e di cui al D.lgs. 74/2000 è necessario dare seguito ai controlli specifici indicati e alle relative misure comportamentali:

- i beni e/o servizi oggetto del contratto siano effettivamente venduti all'altra parte coinvolta e indicata nel documento sotteso al servizio, secondo le modalità, i termini e le condizioni concordate. In caso contrario, darne immediata comunicazione al responsabile di funzione e, nei casi più gravi, all'AD;
- degli acquisti o delle vendite, dei servizi resi o acquisiti sia conservata adeguata traccia documentale, a cura del responsabile interessato, con archiviazione dei relativi documenti, presso la sede della società, sia in formato cartaceo che elettronico;
- i pagamenti eseguiti o ricevuti o ricevuti a titolo di corrispettivo siano conformi:
  - alle vendite/servizi effettivamente resi/ricevuti nonché alle pattuizioni contenute nelrelativo contratto;
  - tutti i pagamenti siano effettuati dietro emissione di fattura o documento equipollente, ove richiesto dalla legge;
    tutti i pagamenti siano regolarmente contabilizzati conformemente alle disposizioni di legge applicabili;
- si deve rispettare il divieto di effettuare pagamenti a fornitori e collaboratori esterni in un paese terzo, diverso da quello delle parti o di esecuzione del contratto, o comunque che si trovi in un paese della black list.

Si devono inoltre prevedere le seguenti condizioni nelle operazioni commerciali:

- tracciabilità dell'operazione tramite documentazione e archiviazione (telematica e/o cartacea) di ogni attività del processo da parte della funzione coinvolta;
- utilizzo del sistema informatico dedicato per la registrazione delle fatture attive e passive, nonché di ogni altro accadimento economico;
- diniego all'accettazione di pagamenti o incassi di contanti, salvo che vi sia espressa autorizzazione da parte della Direzione della società e comunque per importo che non superino somme gestite attraverso la piccola cassa.

Si deve inoltre prevedere che:
1) la società deve avvalersi solo di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;
2) sono preventivamente stabiliti, in funzione della natura della prestazione svolta, limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della società. Il rimborso delle spese sostenute deve essere richiesto attraverso lacompilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute;
3) le risorse finanziarie ottenute come contributo, sovvenzione o finanziamento pubblico devono essere destinate esclusivamente alle iniziative e al conseguimento delle finalità per le quali sono state richieste ed ottenute;
4) l'impiego di tali risorse è sempre motivato dal soggetto richiedente, che ne attesta la coerenza con le finalità per le quali il finanziamento è stato richiesto e ottenuto.

Si dovrà inoltre verificare:
1) la regolamentazione ed il monitoraggio degli accessi al sistema informatico;
2) la contabilizzazione da parte dell'ufficio responsabile delle sole fatture attive/passive che hanno ricevuto il benestare alla registrazione e al loro pagamento/incasso solo dopo aver ricevuto il benestare del responsabile di funzione;
3) la rilevazione di tutti i fatti amministrativi aziendali che hanno riflesso economico e patrimoniale;
4) il corretto trattamento fiscale delle componenti di reddito, detrazioni e deduzioni secondoquanto previsto dalla normativa fiscale;
5) il rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette e indirette;
6) la diffusione delle principali novità normative in materia fiscale al personale coinvolto nellagestione della fiscalità;
7) la verifica con un consulente terzo di qualsivoglia implicazione fiscale derivante dalla esecuzione di una operazione avente carattere ordinario o straordinario. Inoltre, ai fini della corretta gestione degli incassi, al personale è fatto obbligo di segnalare alla Direzione eventuali clienti/fornitori che effettuano operazioni sospette all'atto dell'acquisizione di informazioni (quali ad esempio dichiarazione di ragioni sociali inesistenti, richiesta di pagamenti illeciti e/o fuori campo IVA, emissione di documenti fiscali non corretti, proposta di pagamenti tramite regalie ecc…).