COSEPURI

COSEPURI SOC.COOP.P.A.

Modello di Organizzazione e di gestione ex Decreto Legislativo 8 giugno 2001 n. 231

PARTE SPECIALE

Rev. 4 del 08/02/2013

SOMMARIO

1 INTRODUZIONE

La Parte Speciale si compone di quattro sezioni:

- **ALLEGATO 'A'**, riguardante la tipologia dei reati nei rapporti con la Pubblica Amministrazione (articoli 24 e 25 del D.Lgs. 231/2001);
- **ALLEGATO 'B'**, riguardante i reati informatici (articolo 24bis del D.Lgs. 231/2001).
- **ALLEGATO 'C'**, riguardante i reati societari e gli abusi di mercato (articoli 25ter, 25sexies del D.Lgs. 231/2001 e 187quinquies D.Lgs. 58/1998).
- **ALLEGATO 'D'**, riguardante i reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle normative antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (articolo 25 septies del D.Lgs 231/01)
- **ALLEGATO 'E',** riguardante i reati ambientali

La Parte Speciale affronta queste fattispecie di reato, fra tutte quelle elencate nella Parte Generale, in quanto queste sono state ritenute rientrare nelle aree a rischio di reato in relazione all'attività svolta da Cosepuri.

1.1 Obiettivi della parte speciale

La presente Parte Speciale fa riferimento ai comportamenti posti in essere dagli Operatori Cosepuri come già richiamati nella Parte Generale, nonché dai consulenti, collaboratori esterni e fornitori dell'Ente.

Obiettivo specifico di questa Parte Speciale è quello di far sì che i destinatari adottino e rispettino tutte quelle regole di condotta conformi al Decreto al fine di prevenire i reati in esso indicati.

In particolare vengono qui di seguito richiamate le procedure da osservare ai fini della corretta applicazione del Modello, nonché gli strumenti necessari per l'esercizio delle attività di controllo, monitoraggio e verifica.

2 ALLEGATO 'A': REATI CONTRO LE PUBBICHE AMMINISTRAZIONI

2.1 Tipologia dei reati nei rapporti con la Pubblica Amministrazione (articoli 24 e 25 del D.Lgs. 231/2001)

Preliminarmente si fornisce una sintetica descrizione dei reati contemplati nella presente Parte Speciale "A", coincidente con quelli indicati negli articoli 24 e 25 del Decreto.

- ***Malversazione a danno dello stato o dell'unione europea (articolo 316 bis del Codice Penale)***

Questa ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate.

In particolare, la condotta rilevante consiste nell'avere sottratto, anche parzialmente, la somma ottenuta (finanziamenti, contributi ecc.), a nulla rilevando il fatto che l'attività programmata si sia comunque svolta.

Tenuto conto che il momento consumativo del reato, che coincide con la fase esecutiva cioè nel momento successivo dell'utilizzazione del finanziamento, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che nell'attualità non vengano destinati alle finalità per le quali erano stati erogati.

Esempio: un contributo, in conto interessi o a fondo perduto, per l'acquisto di un'attrezzatura che venga destinato per uno scopo diverso rispetto a quello per il quale era stato concesso.

- **Indebita percezione di erogazioni in danno dello stato o dell'unione europea (articolo 316-ter del Codice Penale)**

L' ipotesi di reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute, si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Unione Europea.

In questo caso, a differenza dell'ipotesi di cui al precedente art. 316 bis c.p. (Malversazione), è irrilevante l'uso che venga fatto delle erogazioni, poiché il reato si consuma nel momento stesso dell'ottenimento dei finanziamenti.

Si tratta di un'ipotesi di reato residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

La differenza tra l'indebita percezione di erogazioni (316ter c.p.) e la truffa aggravata per il conseguimento di erogazioni (640bis c.p.) è rappresentata dal fatto che nella seconda ipotesi l'esposizione non veritiera di documentazione e/o di fatti ovvero l'omissione di informazioni dovute prevista per l'ipotesi di indebita percezione di erogazioni a danno dello Stato è accompagnata da un'attività fraudolenta che va oltre alla semplice ipotesi prevista dall'art. 316ter c.p.

Esempio: nella richiesta di erogazione di contributi, si producono attestazioni false tali da conseguire un finanziamento non dovuto.

- **Concussione (articolo 317 del Codice Penale)**

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli.

In particolare, la condotta penalmente rilevante potrebbe ravvisarsi, nell'ambito di applicazione del Decreto stesso, nell'ipotesi in cui un dipendente o un dirigente della Società concorrano nel reato del pubblico ufficiale, il quale, profittando di tale qualità, richieda a terzi prestazioni non dovute, risultando da tali comportamenti vantaggio per la Società.

In questo caso, non vi è alcun accordo tra le parti ma una volontà prevaricatrice e condizionante del pubblico agente.

Esempio: il pubblico ufficiale, profittando della sua qualità, richiede somme non dovute al fine di concedere vantaggi all'Ente.

- **Corruzione per un atto d'ufficio o contrario ai doveri di ufficio (articoli 318 e 319 del Codice Penale)**

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio, determinando un vantaggio in favore dell'offerente.

L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ipotesi di corruzione impropria - ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ipotesi di corruzione propria – ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

La corruzione, che si può ulteriormente distinguere in antecedente (qualora il denaro non dovuta è corrisposto prima – 318 comma 1 c.p.: corruzione impropria antecedente) o susseguente (qualora il denaro non dovuto è corrisposto dopo – 318 comma 2 c.p.: corruzione impropria susseguente) si differenzia dalla concussione in quanto tra corrotto e corruttore esiste un

accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Esempio: nell'ambito di una gara, un pubblico ufficiale accetta denaro al fine di garantire l'aggiudicazione della stessa.

- **Istigazione alla corruzione (articolo 322 del Codice Penale)**

L'istigazione alla corruzione si configura tutte le volte in cui il reato di corruzione non si perfeziona in quanto il pubblico ufficiale rifiuta l'offerta o la promessa illecita avanzatagli.

Esempio: nell'ambito di una gara, un pubblico ufficiale NON accetta denaro al fine di garantire l'aggiudicazione della stessa.

- **Corruzione in atti giudiziari (articolo 319ter del Codice Penale)**

Il reato si configura nel caso in cui la Società sia parte in un procedimento giudiziario e corrompa un pubblico ufficiale(che può essere, oltre che un magistrato, anche un cancelliere o altro funzionario)al fine di ottenere un vantaggio nel procedimento stesso.

Esempio: nell'ambito di un procedimento giudiziario nel quale l'Ente è parte, si corrompe un magistrato o un cancelliere, al fine di ottenere un vantaggio nel medesimo procedimento.

- **Truffa in danno dello stato, di altro ente pubblico o dell'unione europea (articolo 640 comma 2 n. 1 del Codice Penale)**

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore o da arrecare danno allo Stato (oppure ad altro Ente Pubblico all'Unione Europea).

Esempio: nella partecipazione ad una gara, con artifici e raggiri si forniscono alla P.A. informazioni non veritiere allo scopo di ottenere l'aggiudicazione della gara stessa.

- **Truffa aggravata per il conseguimento di erogazioni pubbliche (articolo 640 bis del Codice Penale)**

Tale ipotesi di reato si configura nel caso in cui la truffa di cui all'art. 640 comma 2 n. 1 c.p.) sia posta in essere per conseguire indebitamente erogazioni pubbliche.

L'art. 640 bis è dunque un'ipotesi più specifica rispetto a quella di cui all'art. 640 comma 2 n. 1 c.p.

Esempio: è l'ipotesi in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

- **Frode informatica in danno dello stato o di altro ente pubblico (articolo 640ter del Codice Penale)**

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danni a terzi.

Esempio: alterazione e violazione di un sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello dovuto.

2.2 Aree a Rischio

In relazione a quanto sopra e compatibilmente con quanto già riportato nella Parte Generale del presente Modello, vengono considerate (ai fini della presente Parte Speciale, Allegato "A")le seguenti aree di attività rischio:

1. gestione delle procedure di gara e/o di negoziazione diretta indette da Enti Pubblici per l'assegnazione di commesse (appalto, fornitura o servizi);

2. gestione delle procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego;

3. gestione delle procedure di sponsorizzazione a favore delle Pubbliche Amministrazioni;

4. gestione delle assunzioni;

5. gestione delle donazioni ad Enti pubblici;

6. gestione dei rapporti con Enti Pubblici ed Autorità in occasione di verifiche, controlli, ispezioni ed accertamenti (giudiziari, tributari, amministrativi, ambientali, sicurezza sul lavoro, ecc) nonché nelle fasi di contenzioso giudiziale in generale ed in quella stragiudiziale con soggetti pubblici ;

7. gestione delle altre "attività sensibili".

L'integrazione delle suddette aree di attività a rischio potrà essere disposta dall'Organo Amministrativo, su eventuale indicazione dell'Organismo di Vigilanza, il quale individuerà le relative ipotesi e definirà gli opportuni provvedimenti operativi.

2.3 Principi e comportamenti per la prevenzione dei reati con la Pubblica Amministrazione.

La presente Parte Speciale Allegato "A" prevede l'espresso divieto, a carico degli Operatori Cosepuri, di tenere le seguenti condotte:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);

2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3. porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Oltre a quanto previsto e ribadito nel Codice Etico di Cosepuri, nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:

a. prendere contatto diretto con l'Ente pubblico al fine di ottenere informazioni circa gli appalti e il rilascio/rinnovo delle licenze e autorizzazioni amministrative al di fuori di specifici incarichi.

b. effettuare elargizioni in denaro a pubblici funzionari;

c. distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (e quindi non eccedente le normali pratiche commerciali o di cortesia) o comunque rivolti ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. Gli omaggi consentiti si debbono sempre caratterizzare per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio la distribuzione di libri d'arte) ovvero l'immagine della Società. I regali offerti, salvo quelli che non hanno un valore economico apprezzabile, debbono essere documentati in modo adeguato per consentire le prescritte verifiche;

d. accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste dal precedente punto b);

e. effettuare prestazioni in favore di Partner che non trovino adeguata giustificazione nel contesto del rapporto collaborativo con gli stessi;

f. riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;

g. presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

h. destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Ai fini dell'attuazione dei comportamenti di cui sopra:

1. devono essere gestiti in modo unitario, procedendo alla standardizzazione delle procedure, i rapporti nei confronti della Pubblica Amministrazione per le suddette aree di attività a rischio;

2. devono essere assunte adeguate informazioni sugli enti nel momento in cui se ne viene in contatto per la prima volta;

3. devono essere assunte adeguate informazioni sulla natura e qualifica degli interlocutori;

4. devono essere assunte adeguate informazioni di dimensione sui fabbisogni dell'Ente con cui si contrae;

5. devono essere assunte adeguate informazioni su eventuali soci, funzionari o dipendenti che abbiano anche cariche pubbliche;

6. devono essere definiti per iscritto gli accordi di associazione con i Partner, evidenziando tutte le condizioni di ciascun accordo e in particolare di quelle economiche;

7. devono essere redatti per iscritto gli incarichi conferiti ai Collaboratori esterni, con l'indicazione del compenso pattuito;

8. non si devono effettuare per cassa o in natura pagamenti di importo superiore a Euro 3.000,00;

9. le dichiarazioni rese a organismi pubblici nazionali comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi del tutto veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;

10. coloro che svolgono una funzione di controllo su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione all'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;

2.4 Protocolli operativi specifici per la prevenzione dei reati derivanti dal rapporto con la Pubblica Amministrazione.

L'analisi dei processi aziendali ha individuato le principali aree a rischio di reato sopra descritte.

Il sistema organizzativo di controllo ha consentito di individuare, per Cosepuri, le seguenti regole:

1. Nell'ambito delle procedure di gara e/o di negoziazione diretta indette da Enti Pubblici per l'assegnazione di commesse (appalto, fornitura o servizi) ci si deve attenere alla procedura aziendale P7.2-01: "Riesame del contratto";

2. nell'ambito della partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti pubblici ed il loro concreto impiego ci si deve attenere al Protocollo A1 " Finanziamenti pubblici";

3. nell'ambito della procedura di sponsorizzazione ci si deve attenere al Protocollo A2:"Sponsorizzazioni a favore della Pubblica Amministrazione";

4. nell'ambito della selezione di personale dipendente ci si deve attenere al Protocollo A4 " Assunzione del personale";

5. nell'ambito delle donazioni ad Enti pubblici ci si deve attenere al Protocollo A5 "Donazioni ad Enti pubblici";

6. nell'ambito delle ispezioni e verifiche da parte di Enti e/o Autorità Pubbliche e nella gestione di contenziosi giudiziali in generale nonché di quelli stragiudiziali nei confronti di soggetti pubblici ci si deve attenere al Protocollo A7 " Gestione dei rapporti con Enti Pubblici ed Autorità in occasione di verifiche, controlli e accertamenti e nella gestione di contenziosi giudiziali e stragiudiziali", allegato al presente Modello;

2.5 Controlli dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organo di Vigilanza di attivarsi con specifici controlli, anche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività sensibili, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole e ai principi del modello.

In ragione dell'attività di vigilanza attribuitagli, si garantisce all'Organismo di Vigilanza libero accesso a tutta la documentazione aziendale rilevante.

3 ALLEGATO 'B': REATI INFORMATICI

3.1 Tipologie di reati informatici (articolo 24bis del Decreto)

Preliminarmente si fornisce una sintetica descrizione dei reati contemplati nella presente Parte Speciale "B", coincidente con quelli indicati nell' articolo 24 bis del Decreto.

1. **Falsità in un documento informatico pubblico o privatro (articolo 491bis del codice penale);**

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Il reato si configura nella falsità concernente direttamente i dati o le informazioni dotati, già di per sé, di efficacia probatoria relativa a programmi specificatamente destinati ad elaborarli indipendentemente da un riscontro cartaceo. Si chiarisce inoltre nella norma che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

2. **Accesso abusivo ad un sistema informatico o telematico (articolo 615 ter del codice penale)**

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

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

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

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza

pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi un'effettiva lesione alla stessa.

3. **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (articolo 615 quater del codice penale)**

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno,abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617quater.

4. **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615 quinquies del codice penale)**

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

5. **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617 quater del codice penale)**

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

primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

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

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

6. **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (articolo 617 quinquies del codice penale)**

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

7. **Danneggiamento di informazioni, dati e programmi informatici (articolo 635 bis del codice penale)**

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

8. **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635 ter del codice penale)**

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione, o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il

fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata.

9. **Danneggiamento di sistemi informatici o telematici (articolo 635 quater del codice penale)**

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

10. **Danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635 quinquies del codice penale)**

Se il fatto di cui all'art.635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

In generale da notare che si parla di danneggiamento informatico quando, considerando la componente hardware e software, interviene una modifica tale da impedirne il funzionamento, anche solo parziale.

11. **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (articolo 640 quinquies del codice penale)**

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00.

3.2 Aree a rischio

Tenuto conto dell'attività svolta dalla Società, sebbene i delitti informatici e il trattamento illecito dei dati siano reati solo astrattamente ipotizzabili, dall'analisi dei processi, compatibilmente con quanto già riportato nella Parte Generale del presente Modello, vengono considerate (ai fini della presente Parte Speciale, Allegato "B") le seguenti aree di attività rischio:

1. gestione delle procedure di accesso alla rete intranet e internet;

2. gestione delle procedure di back up dei dati e loro conservazione;

3. gestione delle altre “attività sensibili”.

L'integrazione delle suddette aree di attività a rischio potrà essere disposta dall’Organo Amministrativo, su eventuale indicazione dell’Organismo di Vigilanza, il quale individuerà le relative ipotesi e definirà gli opportuni provvedimenti operativi.

3.3 Principi e comportamenti per la prevenzione dei reati informatici

La presente Parte Speciale Allegato “B” prevede l'espresso divieto, a carico degli Operatori Cosepuri di tenere le seguenti condotte:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24bis del Decreto);

2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

Oltre a quanto previsto e ribadito nel Codice Etico di Cosepuri, nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:

a. accedere abusivamente al sistema informatico o telematico sia di soggetti pubblici che privati;

b. accedere al proprio sistema informatico o telematico con l’intento di alterare e/o cancellare dati e/o informazioni in maniera abusiva;

c. installare nella rete aziendale un software non rientrante nello scopo per cui il sistema informatico è stato assegnato all’utente, al fine sia di evitare il rallentamento o il blocco della rete informatica aziendale che per impedire o interrompere o danneggiare le comunicazioni informatiche aziendali ovvero l’intero sistema informatico aziendale;

d. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

e. effettuare attività di intercettazione fraudolenta, interruzione o impedimento di comunicazioni relative a un sistema informatico o telematico, al fine di acquisire informazioni riservate;

f. utilizzare e detenere abusivamente ogni mezzo idoneo all'accesso ad un sistema informatico o telematico (codici e password), al fine di acquisire informazioni riservate;

g. istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

h. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

i. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

j. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

Pertanto, i soggetti sopra indicati devono:

1. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi e utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;

2. informare tempestivamente il Responsabile dei Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta nel caso di smarrimento o furto di apparecchiatura informatica;

3. evitare di lasciare incustodito e/o accessibile ad altri il proprio computer;

4. evitare che altre persone (familiari, amici, ecc) utilizzino il proprio computer;

5. utilizzare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;

6. utilizzare la connessione a Internet solo per gli scopi necessari all'attività lavorativa;

7. evitare l'utilizzo di password di altri utenti aziendali

8. custodire diligentemente la propria password (non rivelarla a nessuno, non trascriverla,ecc)

9. introdurre e/o conservare in azienda, sia in forma cartacea che digitale documentazione e/o materiale informatico di natura riservata e di proprietà di terzi solo con il loro espresso consenso

10. evitare l'utilizzo di applicazioni/software che non siano state preventivamente approvate dal Responsabile Sistemi Informativi o la cui provenienza sia dubbia;

11. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;

12. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

13. segnalare prontamente alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

14. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

15. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

3.4 Protocolli operativi specifici per la prevenzione dei reati informatici

Nel *Documento Programmatico sulla Sicurezza* sono analizzate le situazioni aziendali ed organizzate le procedure a garanzia della sicurezza nei trattamenti dei dati.

In particolare, per quel che riguarda il rischio analizzato nel presente capitolo, è svolta l'analisi:

- dei server;
- delle misure di sicurezza per i trattamenti informatici;
- degli strumenti antivirus;
- dei sistemi anti-intrusione;
- dei firewall;
- dei piani di Disaster Recovery.

Per quanto riguarda le modalità operative per il corretto svolgimento delle attività ed il raggiungimento degli obiettivi sopra indicati si rimanda a quanto

definito nel Documento programmatico sulla sicurezza relativamente alle istruzioni specifiche fornite agli incaricati, in particolare:

- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornire copia al preposto alla custodia della parola chiave;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali

3.5 Controlli dell'Organismo di Vigilanza

Dal momento che l'Organismo di Vigilanza lavorerà in stretta collaborazione con le funzioni preposte ai Sistemi Informativi, dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'organismo stesso.

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili.

Di detti controlli l'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale, secondo le modalità previste nella Parte Generale del presente Modello.

4 ALLEGATO "C": REATI SOCIETARI

4.1 Tipologie dei reati societari (articolo 25ter del Decreto)

E' opportuno fornire una breve descrizione dei reati contemplati nel presente Parte Speciale Allegato "C", coincidente con quelli indicati negli articoli 25ter del Decreto, raggruppandoli, per maggiore chiarezza, in 3 tipologie differenti.

4.1.1 Falsità in comunicazioni, prospetti e relazioni

- **False comunicazioni sociali (articoli 2621 e 2622 del Codice Civile)**

Si tratta di due ipotesi di reato la cui condotta tipica coincide quasi totalmente e che si differenziano per il verificarsi (art. 2622 c.c.) o meno (art. 2621 c.c.) di un danno patrimoniale nei confronti dei soci o dei creditori. Questi reati si realizzano tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero mediante l'omissione nei medesimi documenti di informazioni, la cui comunicazione è imposta dalla legge, riguardo alla situazione economica, patrimoniale o finanziaria della Società. La condotta che può essere commissiva od omissiva deve essere realizzata in entrambi i casi con l'intenzione di ingannare i soci o il pubblico. La condotta deve inoltre risultare idonea a trarre in errore i destinatari delle indicate comunicazioni sociali, essendo in definitiva rivolta a conseguire un ingiusto profitto a beneficio dell'autore del reato ovvero di terzi.

Si precisa che le informazioni false o omesse devono essere tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della Società.

Per il reato di cui all'articolo 2622 c.c. è prevista la procedibilità a querela di parte, salvo che sia commesso in danno dello Stato, di altri enti pubblici, dell'Unione Europea o che si tratti di società quotate, nel qual caso è prevista la procedibilità d'ufficio.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari e i liquidatori.

Esempio: il Consiglio di Amministrazione ignora l'indicazione del Direttore Amministrativo circa l'esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti ed iscrive un ammontare di crediti superiore al dovuto al fine di non fare emergere una perdita.

- **Falso in prospetto (articolo 173 bis D.Lgs. 58/98)**

Tale ipotesi di reato consiste nell'esporre false informazioni ovvero nell'occultare dati o notizie all'interno dei prospetti (per tali intendendosi i documenti richiesti ai fini della sollecitazione all'investimento) secondo modalità idonee ad indurre in errore i destinatari dei prospetti stessi.

Si precisa che deve sussistere l'intenzione di ingannare i destinatari dei prospetti e che la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.

Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

Esempio: il Consiglio di Amministrazione omette consapevolmente di rappresentare in un documento informativo richiesto per legge elementi idonei a formare un giudizio veritiero.

4.1.2 Tutela penale del capitale sociale

- **Indebita restituzione dei conferimenti (articolo 2626 del Codice Civile)**

Tale ipotesi di reato consiste nel procedere, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli. Il delitto si perfeziona con la lesione dell'integrità e dell'effettività del capitale sociale a tutela dei diritti dei creditori e dei terzi. Soggetti attivi del reato possono essere solo gli amministratori. La legge, cioè, non ha inteso punire i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

Esempio: l'Assemblea della Società, su proposta del Consiglio di Amministrazione, delibera la compensazione di un debito del socio nei confronti della Società con il credito da conferimento che quest'ultima vanta nei confronti del socio stesso, attuando una restituzione indebita dei conferimenti.

- **Illegale ripartizione degli utili o delle riserve (articolo 2627 del Codice Civile)**

Tale ipotesi di reato consiste nella ripartizione di "utili" (o acconti sugli "utili") non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche costituite con "utili") che non possono essere distribuite. Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato. Soggetti attivi del reato sono gli amministratori. La legge cioè non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso

eventuale, in virtù del quale risponderanno del reato anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

Esempio: l'Assemblea della Società, su proposta del Consiglio di Amministrazione, delibera la distribuzione di dividendi che costituiscono, non un utile di esercizio, ma fondi non distribuibili perché destinati per legge a riserva legale.

- **Operazioni in pregiudizio dei creditori (articolo 2629 del Codice Civile)**

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

- **Indebita ripartizione dei beni sociali da parte dei liquidatori (articolo 2633 del Codice Civile)**

Tale ipotesi di reato consiste nella ripartizione, durante la fase di liquidazione della società, di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Soggetti attivi del reato sono esclusivamente i liquidatori.

4.1.3 Tutela penale del regolare funzionamento della società

- **Impedito controllo (articolo 2625 del Codice Civile)**

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti o altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione, qualora tale condotta abbia cagionato un danno ai soci. Tale previsione normativa prevede un illecito di natura amministrativa, e come tale non suscettibile di rilevanza ai fini del D.Lgs. 231/2001, salvo che venga cagionato un danno ai soci. Solo in quest'ultimo caso trova applicazione la disciplina della responsabilità dell'ente dipendente da reato.

L'illecito può essere commesso esclusivamente dagli amministratori.

Esempio: un funzionario della Società rifiuta di fornire al Collegio Sindacale i documenti richiesti per l'espletamento dell'incarico, quali, ad esempio, quelli concernenti le azioni legali intraprese dalla Società per il recupero crediti.

- **Illecita influenza sull' assemblea (articolo 2636 del Codice Civile)**

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

Esempio: il Consiglio di Amministrazione della Società, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinante anche del socio di maggioranza, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria.

4.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra descritte le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale Allegato "C" del Modello, le seguenti:

1. redazione del bilancio;
2. predisposizione di comunicazioni dirette ai soci riguardo alla situazione economica, patrimoniale e finanziaria della Società;
3. gestione dei rapporti con il Collegio Sindacale;
4. predisposizione e divulgazione verso l'esterno di dati o notizie (ulteriori rispetto a quelli di cui al punto 1. relativi alla Società);
5. predisposizione di comunicazioni ad Autorità pubbliche di Vigilanza;
6. gestione delle fatture;
7. gestione del recupero crediti;
8. gestione delle operazioni di cassa;
9. gestione degli acquisti;
10. gestione della contabilità generale soci/appaltatori;
11. altre "attività sensibili".

L'integrazione delle suddette aree di attività a rischio potrà essere disposta dall'Organo Amministrativo, su eventuale indicazione dell'Organismo di Vigilanza, il quale individuerà le relative ipotesi e definirà gli opportuni provvedimenti operativi.

4.3 Principi e comportamenti per la prevenzione dei reati in materia societaria

La presente Parte Speciale Allegato "C" prevede, a carico degli Operatori Cosepuri di tenere le seguenti condotte:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti reati societari;

2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società. In ordine a tale punto, è fatto divieto di:

    - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;

    - omettere di comunicare dati e informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;

4. osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità del capitale sociale ed agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere. In ordine a tale punto, è fatto divieto di:

    - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

    - ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;

    - effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;

- procedere in ogni modo la formazione o aumento fittizi del capitale sociale;

- ripartire i beni sociali tra i soci in fase di liquidazione prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;

5. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge. In ordine a tale punto, è fatto divieto di:

    - tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o revisione della gestione sociale da parte del Collegio Sindacale;

    - porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento

4.4 Protocolli operativi specifici per la prevenzione dei reati societari

Le procedure gestionali afferenti la movimentazione in entrata e uscita di risorse finanziarie dovranno essere integrate e aggiornate dall'Organismo di Vigilanza in ordine alla prevenzione dei reati previsti dal D.Lgs. 231/2001.

I controlli saranno finalizzati per esempio alla rilevazione di pagamenti o incassi di corrispettivi non coerenti con l'operazione cui si correlano al fine di appurare l'eventuale presenza implicita di poste extracontabili.

Nell'ambito della gestione delle risorse finanziarie e più in generale nella movimentazione in entrata e uscita di risorse finanziarie, ci si deve attenere a quanto riportato nel fascicolo "Organizzazione e procedure dell'area amministrativa". In particolare:

1. "Ufficio fatturazione";

2. "Ufficio recupero crediti-gestione amministrativa del personale";

3. "Ufficio cassa";

4. "Ufficio acquisti/servizi generali".

5. "Ufficio contabilità generale - soci/appaltatori".

Oltre alle modalità di gestione delle risorse finanziarie, si indicano i seguenti Protocolli:

4.4.1 Protocolli specifici su comunicazioni e prospetti

Tali procedure tendono ad impedire la commissione dei reati previsti dal D.Lgs. 231/2001 derivanti da comunicazioni dirette ai soci ovvero al pubblico in generale riguardo alla situazione economica, patrimoniale e finanziaria della Società.

Si indicano qui di seguito alcune procedure specifiche che devono essere rispettate da tutti i destinatari a integrazione delle altre procedure aziendali esistenti e alla matrice interna di controllo dell'Organismo di Vigilanza:

1. Nelle attività di predisposizione delle comunicazioni indirizzate ai soci il Responsabile Amministrativo deve mettere tempestivamente a disposizione di tutti i componenti del Consiglio di Amministrazione la bozza del bilancio, prima della riunione per l'approvazione.

2. Gli Amministratori, i dirigenti e i dipendenti di Cosepuri e delle Società da essa controllate sono obbligati a:

    - mantenere la segretezza circa le informazioni di carattere riservato;

    - trattare tali informazioni solo nell'ambito di canali autorizzati, adottando ogni necessaria cautela affinché la relativa circolazione nel contesto aziendale possa svolgersi senza pregiudizio del carattere riservato delle informazioni stesse;

3. I sindaci di Cosepuri e/o delle Società controllate sono tenuti a mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei loro compiti. Ogni rapporto dei sindaci con terzi, che coinvolga documenti e informazioni riservati concernenti Cosepuri potrà avvenire solo previa consultazione con il Presidente di Cosepuri.

4. Per tutte le informazioni che siano state diffuse senza il rispetto della presente procedura provvedere all'immediata puntualizzazione nella stessa forma e metodo in cui l'informazione è stata data anche mediante smentita della stessa.

4.4.2 Protocolli specifici per i rapporti con il Collegio Sindacale

Tali procedure tendono ad impedire la commissione dei reati previsti dal D. Lgs. 231/2001 derivanti dalla gestione dei rapporti con il Collegio Sindacale.

Si indicano qui di seguito alcune procedure specifiche che devono essere rispettate da tutti i destinatari a integrazione delle altre procedure aziendali esistenti e alla matrice interna di controllo dell'Organismo di Vigilanza.

Nella predisposizione di comunicazioni al Collegio Sindacale e gestione dei rapporti con lo stesso occorrerà porre particolare attenzione al rispetto:

a. delle disposizioni di legge;

b. degli obblighi di collaborazione da fornire nel corso delle verifiche periodiche e non.

Le procedure da osservare per garantire il rispetto di quanto precedentemente espresso dovranno essere conformi ai seguenti criteri:

1. dovrà essere data attuazione a tutti gli interventi di natura organizzativo-contabile necessari a garantire che il processo di acquisizione ed elaborazione di dati ed informazioni assicuri la corretta e completa predisposizione delle comunicazioni;

2. dovrà essere data adeguata evidenza delle procedure seguite in attuazione di quanto richiesto al precedente punto, con particolare riferimento all'individuazione dei responsabili che hanno proceduto alla raccolta e all'elaborazione dei dati e delle informazioni ivi previste;

4.5 Controlli dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

a. curare l'emanazione e l'aggiornamento di istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle attività a rischio, come individuate nella presente Parte Speciale Allegato "C". Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

b. con riferimento al bilancio, alle relazioni e alle altre comunicazioni sociali previste dalla legge, l'Organismo di Vigilanza provvede all'espletamento dei seguenti compiti:

    - monitoraggio sull'efficacia delle procedure interne per la prevenzione del reato di false comunicazioni sociali;

    - esame di eventuali segnalazioni specifiche pervenute ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;

    - vigilanza sull'effettiva sussistenza delle condizioni per garantire al Collegio Sindacale una concreta autonomia nelle sue funzioni di controllo delle attività aziendali;

- mantenere un flusso informativo costante tra l'Organismo di Vigilanza e gli amministratori e/o sindaci, ai quali compete convocare l'assemblea dei soci per i provvedimenti conseguenti dato che, si ricorda, il controllo ultimo sull'operato degli amministratori viene svolto dal socio, sul cui patrimonio le sanzioni incidono direttamente;

c. con riferimento alle altre attività a rischio:

- verifiche periodiche sul rispetto delle procedure interne;
- monitoraggio sull'efficacia delle verifiche atte a prevenire la commissione dei reati;
- esame di eventuali segnalazioni specifiche pervenute ed effettuazione degli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- verificare a campione se tutte le operazioni aziendali siano documentabili e verificabili;

5 ALLEGATO "D": REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORMATIVE ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

5.1 Tipologia di reati in materia di sicurezza e salute sul lavoro (articolo 25 septies del D.Lgs 231/01)

Preliminarmente si fornisce una sintetica descrizione dei reati contemplati nella presente Parte Speciale "D", coincidente con quelli indicati nell' articolo 25 septies del Decreto introdotti dalla Legge 3 agosto 2007, n.123.

1. Omicidio colposo (articolo 589 del Codice Penale)

Tale ipotesi di reato si configura nel caso in cui si cagioni la morte di una persona.

In particolare, ai fini dell'integrazione del reato, non è richiesta la coscienza e la volontà di cagionare l'evento lesivo ma, la condotta penalmente rilevante si ravvisa anche per mera negligenza, imprudenza o imperizia del soggetto agente, ovvero l'inosservanza, da parte di quest'ultimo di leggi, regolamenti, ordini o discipline.

2. Lesioni colpose gravi o gravissime (articolo 590 del Codice Penale)

Tale ipotesi di reato si configura nel caso in cui si cagionino lesioni gravi o gravissime a una persona.

Per lesioni gravi si intendono:

- Dal fatto ne deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore a quaranta giorni;
- Dal fatto ne deriva un indebolimento permanente di un senso o di un organo.

Per lesioni gravissime si intendono:

- Dal fatto ne deriva una malattia certamente o probabilmente insanabile;
- Dal fatto ne deriva la perdita di un senso, di un arto, dell'uso di un organo, della capacità di procreare, ecc;
- Dal fatto ne deriva un mutilazione che renda l'arto inservibile;

- Dal fatto ne deriva la deformazione ovvero lo sfregio permanente del viso.

Anche per questo reato non è necessario che il soggetto agente abbia voluto cagionare l'evento lesivo, ma è sufficiente la mera negligenza, imprudenza o imperizia dello stesso, ovvero l'inosservanza di leggi, regolamenti, ordini o discipline.

Le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche.

5.2 Aree a Rischio

In relazione a quanto sopra e compatibilmente con quanto già riportato nella Parte Generale del presente Modello, vengono considerate (ai fini della presente Parte Speciale, Allegato "D")le seguenti aree di attività rischio:

1. Gestione delle procedure di mappatura dei rischi
2. Gestione delle procedure di sicurezza ex D.Lgs 81/08
3. gestione delle altre "attività sensibili".

L'integrazione delle suddette aree di attività a rischio potrà essere disposta dall'Organo Amministrativo, su eventuale indicazione dell'Organismo di Vigilanza, il quale individuerà le relative ipotesi e definirà gli opportuni provvedimenti operativi.

Con particolare riferimento all'organigramma della sicurezza, all'individuazione, all'analisi dei rischi potenziali e delle relative misure di prevenzione, si rimanda a quanto previsto nel Documento di Valutazione dei Rischi redatto dalla Società ai sensi della normativa prevenzionistica vigente.

5.3 Principi e comportamenti per la prevenzione dei reati in materie di sicurezza e salute sul lavoro

La presente Parte Speciale Allegato "D" prevede che, nello svolgimento delle proprie attività e nei limiti dei rispettivi compiti, funzioni e responsabilità, gli Operatori Cosepuri devono rispettare, oltre alle previsioni ed alle prescrizioni del Modello adottato dalla Società, anche la normativa vigente in materia di salute e sicurezza sul lavoro e le relative procedure aziendali vigenti.

Si riportano di seguito i doveri delle varie figure aziendali come previsto dal D.Lgs.81/08.

5.3.1 Compiti del datore di lavoro (art.17 ex D.Lgs 81/08):

Il datore di lavoro non può delegare le seguenti attività

a) la valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'articolo 28 (del D.Lgs 81/08);

b) la designazione del responsabile del servizio di prevenzione e protezione dai rischi.

Inoltre deve provvedere affinché:

- i luoghi di lavoro siano conformi alle prescrizioni normative vigenti**;**
- le vie di circolazione interne o all'aperto che conducono a uscite o ad uscite di emergenza e le uscite di emergenza siano sgombre allo scopo di consentirne l'utilizzazione in ogni evenienza;
- i luoghi di lavoro, gli impianti e i dispositivi vengano sottoposti a regolare manutenzione tecnica e vengano eliminati, quanto più rapidamente possibile, i difetti rilevati che possano pregiudicare la sicurezza e la salute dei Lavoratori;
- i luoghi di lavoro, gli impianti e i dispositivi vengano sottoposti a regolare pulitura, onde assicurare condizioni igieniche adeguate;
- gli impianti e i dispositivi di sicurezza, destinati alla prevenzione o all'eliminazione dei pericoli, vengano sottoposti a regolare manutenzione e al controllo del loro funzionamento;
- in genere, le misure tecniche, organizzative e procedurali di prevenzione e protezione adottate dalla Società siano adeguate rispetto ai fattori di rischio esistenti. Tale attività di monitoraggio deve essere programmata, con la definizione dei compiti e delle responsabilità esecutive, nonché delle metodologie da seguire, e formalizzata mediante la redazione di appositi piani di monitoraggio;

e deve garantire, nell'ambito della propria attività, il rispetto della normative vigente in materia di:

- scelta, installazione, controllo e manutenzione delle attrezzature, nonché di loro utilizzazione da parte dei Lavoratori;
- uso dei dispositivi di protezione individuale;
- impianti ed apparecchiature elettriche;
- movimentazione manuale di carichi;

- utilizzo di videoterminali;
- prevenzione e protezione contro le esplosioni.

5.3.2 Compiti del datore di lavoro e dei dirigenti (art.18 ex D.Lgs 81/08):

I Datori di Lavoro ed i Dirigenti devono:

a) nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal presente decreto legislativo.

b) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;

c) nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;

d) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;

e) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;

f) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;

g) richiedere al medico competente l'osservanza degli obblighi previsti a suo carico nel presente decreto;

h) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

i) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

l) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37 (ex Dlgs 81/08);

m) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;

n) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;

o) consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r);

p) elaborare il documento di cui all'articolo 26, comma 3, e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza;

q) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;

r) comunicare all'INAIL, in relazione alle rispettive competenze, a fini statistici e informativi, i dati relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, le informazioni relative agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni;

s) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50;

t) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43. Tali misure devono essere adeguate alla natura dell'attività', alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;

u) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro;

v) nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'articolo 35;

w) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

x) comunicare annualmente all'INAIL i nominativi dei rappresentanti dei lavoratori per la sicurezza;

y) vigilare affinche' i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

Il Datore di Lavoro, inoltre, fornisce al RSPP ed al Medico Competente le necessarie informazioni in merito a:

a) la natura dei rischi;

b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;

c) la descrizione degli impianti e dei processi produttivi;

d) i dati di cui alla lett. p) che precede, e quelli relativi alle malattie professionali;

e) i provvedimenti adottati dagli organi di vigilanza.

5.3.3 Compiti dei preposti (art.19 ex D.Lgs 81/08):

I preposti, secondo le loro attribuzioni e competenze, devono:

a) sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di persistenza della inosservanza, informare i loro superiori diretti;

b) verificare affinche' soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;

c) richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinche' i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

d) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

e) astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;

f) segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;

g) frequentare appositi corsi di formazione secondo quanto previsto dall'articolo 37.

5.3.4 Compiti dei lavoratori (art.20 ex D.Lgs 81/08):

I lavoratori hanno l'obbligo di:

1. prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

2. I lavoratori devono in particolare:

a) contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

b) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;

c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;

d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;

e) segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;

f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;

g) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;

h) partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;

i) sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.

5.3.5 Compiti del medico competente (art. 25 ex D.Lgs 81/08):

Il medico competente:

a) collabora con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, all'attività' di formazione e informazione nei confronti dei lavoratori, per la parte di competenza, e alla organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro. Collabora inoltre alla attuazione e valorizzazione di programmi volontari di «promozione della salute», secondo i principi della responsabilità sociale;

b) programma ed effettua la sorveglianza sanitaria di cui all'articolo 41 attraverso protocolli sanitari definiti in funzione dei rischi specifici e tenendo in considerazione gli indirizzi scientifici più avanzati;

c) istituisce, anche tramite l'accesso alle cartelle sanitarie e di rischio, di cui alla lettera f), aggiorna e custodisce, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria. Nelle aziende o unità produttive con più di 15 lavoratori il medico competente concorda con il datore di lavoro il luogo di custodia;

d) consegna al datore di lavoro, alla cessazione dell'incarico, la documentazione sanitaria in suo possesso, nel rispetto delle disposizioni di cui al decreto legislativo del 30 giugno 2003, n. 196, e con salvaguardia del segreto professionale;

e) consegna al lavoratore, alla cessazione del rapporto di lavoro, la documentazione sanitaria in suo possesso e gli fornisce le informazioni riguardo la necessità di conservazione;

f) invia all'ISPESL, esclusivamente per via telematica, le cartelle sanitarie e di rischio nei casi previsti dal presente decreto legislativo, alla cessazione del rapporto di lavoro, nel rispetto delle disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196. Il lavoratore interessato puo' chiedere copia delle predette cartelle all'ISPESL anche attraverso il proprio medico di medicina generale;

g) fornisce informazioni ai lavoratori sul significato della sorveglianza sanitaria cui sono sottoposti e, nel caso di esposizione ad agenti con effetti a lungo termine, sulla necessità di sottoporsi ad accertamenti sanitari anche dopo la cessazione della attività che comporta l'esposizione a tali agenti. Fornisce altresì, a richiesta, informazioni analoghe ai rappresentanti dei lavoratori per la sicurezza;

h) informa ogni lavoratore interessato dei risultati della sorveglianza sanitaria di cui all'articolo 41 e, a richiesta dello stesso, gli rilascia copia della documentazione sanitaria;

i) comunica per iscritto, in occasione delle riunioni di cui all'articolo 35, al datore di lavoro, al responsabile del servizio di prevenzione protezione dai rischi, ai rappresentanti dei lavoratori per la sicurezza, i risultati anonimi collettivi della sorveglianza sanitaria effettuata e fornisce indicazioni sul significato di detti risultati ai fini della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori;

l) visita gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa che stabilisce in base alla valutazione dei rischi; la indicazione di una periodicità diversa dall'annuale deve essere comunicata al datore di lavoro ai fini della sua annotazione nel documento di valutazione dei rischi;

m) partecipa alla programmazione del controllo dell'esposizione dei lavoratori i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della sorveglianza sanitaria;

n) comunica, mediante autocertificazione, il possesso dei titoli e requisiti di cui all'articolo 38 al Ministero della salute entro il termine di sei mesi dalla data di entrata in vigore del presente decreto.

5.3.6 Compiti del servizio prevenzione e protezione (art.33 ex D.Lgs 81/08):

Il servizio prevenzione e protezione provvede:

a) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli

ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;

b) ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2, e i sistemi di controllo di tali misure;

c) ad elaborare le procedure di sicurezza per le varie attività aziendali;

d) a proporre i programmi di informazione e formazione dei lavoratori;

e) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35;

f) a fornire ai lavoratori le informazioni di cui all'articolo 36.

5.3.7 Attribuzioni del Rappresentante dei lavoratori per la sicurezza (art.50 ex D.Lgs 81/08):

Fatto salvo quanto stabilito in sede di contrattazione collettiva, il rappresentante dei lavoratori per la sicurezza:

a) accede ai luoghi di lavoro in cui si svolgono le lavorazioni;

b) e' consultato preventivamente e tempestivamente in ordine alla valutazione dei rischi, alla individuazione, programmazione, realizzazione e verifica della prevenzione nella azienda o unità produttiva;

c) e' consultato sulla designazione del responsabile e degli addetti al servizio di prevenzione, alla attività di prevenzione incendi, al primo soccorso, alla evacuazione dei luoghi di lavoro e del medico competente;

d) è consultato in merito all'organizzazione della formazione di cui all'articolo 37;

e) riceve le informazioni e la documentazione aziendale inerente alla valutazione dei rischi e le misure di prevenzione relative, nonché quelle inerenti alle sostanze ed ai preparati pericolosi, alle macchine, agli impianti, alla organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali;

f) riceve le informazioni provenienti dai servizi di vigilanza;

g) riceve una formazione adeguata e, comunque, non inferiore a quella prevista dall'articolo 37;

h) promuove l'elaborazione, l'individuazione e l'attuazione delle misure di prevenzione idonee a tutelare la salute e l'integrita' fisica dei lavoratori;

i) formula osservazioni in occasione di visite e verifiche effettuate dalle autorità competenti, dalle quali e', di norma, sentito;

l) partecipa alla riunione periodica di cui all'articolo 35;

m) fa proposte in merito alla attività di prevenzione;

n) avverte il responsabile della azienda dei rischi individuati nel corso della sua attività;

o) può fare ricorso alle autorità competenti qualora ritenga che le misure di prevenzione e protezione dai rischi adottate dal datore di lavoro o dai dirigenti e i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.

Il rappresentante dei lavoratori per la sicurezza deve disporre del tempo necessario allo svolgimento dell'incarico senza perdita di retribuzione, nonché dei mezzi e degli spazi necessari per l'esercizio delle funzioni e delle facoltà riconosciutegli, anche tramite l'accesso ai dati, di cui all'articolo 18, comma 1, lettera r), contenuti in applicazioni informatiche. Non può subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei suoi confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

Le modalità per l'esercizio delle funzioni di cui al comma 1 sono stabilite in sede di contrattazione collettiva nazionale.

Il rappresentante dei lavoratori per la sicurezza, su sua richiesta e per l'espletamento della sua funzione, riceve copia del documento di cui all'articolo 17, comma 1, lettera a).

I rappresentanti dei lavoratori per la sicurezza dei lavoratori rispettivamente del datore di lavoro committente e delle imprese appaltatrici, su loro richiesta e per l'espletamento della loro funzione, ricevono copia del documento di valutazione dei rischi di cui all'articolo 26, comma 3.

Il rappresentante dei lavoratori per la sicurezza e' tenuto al rispetto delle disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196 e del segreto industriale relativamente alle informazioni contenute nel documento di valutazione dei rischi e nel documento di valutazione dei rischi di cui all'articolo 26, comma 3, nonché al segreto in ordine ai processi lavorativi di cui vengono a conoscenza nell'esercizio delle funzioni.

L'esercizio delle funzioni di rappresentante dei lavoratori per la sicurezza e' incompatibile con la nomina di responsabile o addetto al servizio di prevenzione e protezione.

5.4 Protocolli operativi specifici per la prevenzione dei reati in materia di Salute e Sicurezza sul lavoro

La gestione delle questioni connesse alla salute e alla sicurezza sul lavoro è effettuata con obiettivo di prevedere sistematicamente :

- L'identificazione dei rischi e la loro valutazione;
- L'individuazione delle misure di prevenzione e protezione adeguate rispetto ai rischi riscontrati affinché questi ultimi siano eliminati ovvero, ove ciò non sia possibile, ridotti al minimo;
- La limitazione al minimo del numero di lavoratori esposti a rischi
- La definizione di adeguate misure di protezione collettiva e individuale
- Il controllo sanitario dei lavoratori in funzione dei rischi specifici
- La programmazione della prevenzione
- La formazione, l'addestramento, la comunicazione adeguati dei destinatari del Modello nei limiti dei rispettivi ruoli, funzioni e responsabilità
- Le regole di manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo alla manutenzione dei dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Per quanto riguarda le modalità operative per il corretto svolgimento delle attività ed il raggiungimento degli obiettivi sopra indicati si rimanda a quanto definito nel documento di valutazione dei rischi e nelle procedure aziendali, redatte in conformità alla normativa prevenzionistica vigente, le quali assicurano l'adeguata tracciabilità dei processi e delle attività svolte.

In particolare:

1. nell'ambito della gestione della mappatura dei rischi ci si deve attenere a quanto previsto nel Documento di Valutazione dei Rischi adottato dalla Società;
2. nell'ambito della gestione delle procedure di sicurezza e nella verifica della loro corretta applicazione, bisogna uniformarsi a quanto previsto nelle apposite procedure aziendali.

5.4.1 Il sistema di monitoraggio della sicurezza

La Società ha rivolto particolare attenzione alla esigenza di predisporre ed implementare, in materia di sicurezza sul lavoro, un efficace ed efficiente sistema di controllo.

Tale sistema di controllo prevede:

1. la registrazione delle verifiche svolte dalla Società attraverso la redazione di appositi verbali

2. un sistema di monitoraggio della sicurezza su due livelli:

a) Monitoraggio svolto direttamente da tutti i soggetti che operano nell'ambito della struttura organizzativa della Società, essendo previsto:

   - I soggetti aziendali con specifici compiti in materia di sicurezza sul lavoro (ad esempio, datore di lavoro, dirigenti, preposti, RSPP,ecc) intervengono in materia di:

     - vigilanza periodica e sistematica sulla osservanza degli obblighi di legge e delle procedure aziendali in materia si sicurezza sul lavoro;

     - segnalazione al datore di lavoro di eventuali deficienze e problematiche;

     - individuazione e valutazione dei fattori aziendali di rischio;

     - elaborazione delle misure preventive e protettive attuate e richiamate nel Documento di Valutazione dei rischi;

     - predisposizione dei programmi di formazione e addestramento dei lavoratori, nonché di comunicazione e coinvolgimento degli stessi.

   - L'autocontrollo dei lavoratori che devono sia utilizzare correttamente le attrezzature di lavoro, le sostanze pericolose e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza e di protezione messi a loro disposizione, sia segnalare immediatamente le deficienze di tali mezzi e dispositivi nonché qualsiasi eventuale condizione di pericolo a cui vengano a conoscenza;

b) Monitoraggio svolto dall'Organismo di Vigilanza al quale è assegnato il compito di verificare la funzionalità del complessivo sistema

preventivo adottato dalla Società a tutela della salute e della sicurezza dei lavoratori. Tale compito è stato assegnato all'OdV in ragione della sua idoneità ad assicurare l'obiettività e l'imparzialità dell'operato, nonché l'indipendenza del settore di lavoro sottoposto a verifica ispettiva.

5.5 Controlli dell'Organismo di Vigilanza

Con riferimento al settore della salute e della sicurezza sul lavoro, l'OdV, pur non ricoprendo un ruolo operativo, deve:

- vigilare sull'adeguatezza e sul rispetto del Modello, inclusi il Codice Etico e le procedure aziendali in materia di salute e sicurezza sul lavoro;

- esaminare le segnalazioni concernenti eventuali violazioni del Modello, ivi incluse le segnalazioni, non riscontrate tempestivamente dai soggetti competenti, concernenti eventuali deficienze o inadeguatezze dei luoghi, delle attrezzature di lavoro, ovvero dei dispositivi di protezione messi a disposizione dalla Società, ovvero riguardanti una situazione di pericolo connesso alla salute ed alla sicurezza sul lavoro;

- monitorare la funzionalità del complessivo sistema preventivo adottato dalla Società con riferimento al settore della salute e della sicurezza sul lavoro, in quanto organismo idoneo ad assicurare l'obiettività, l'imparzialità e l'indipendenza dal settore di lavoro sottoposto a verifica;

- proporre al Consiglio di Amministrazione, ovvero alle funzioni aziendali eventualmente competenti, gli aggiornamenti del Modello, del sistema preventivo adottato dalla Società ovvero delle procedure aziendali vigenti, che si rendessero necessari o opportuni in considerazione di eventuali inadeguatezze riscontrate, ovvero a seguito di significative violazioni o di cambiamenti della struttura organizzativa della Società in relazione al progresso scientifico e tecnologico.

- proporre l'irrogazione di sanzioni disciplinari, per l'ipotesi in cui sia riscontrata la commissione di condotte indicate nel sistema disciplinare adottato dalla Società ai sensi del Decreto.

Al fine di consentire all'Organismo di Vigilanza di svolgere efficacemente le sue mansioni, l'RSPP deve inviare all'OdV copia della reportistica periodica in materia di salute e sicurezza sul lavoro e tutti i dati relativi agli infortuni sul lavoro occorsi nei siti della Società.

6 ALLEGATO 'E': REATI AMBIENTALI

6.1 Tipologia dei reati ambientali (articolo 25 undicies del D.Lgs. 231/2001)

Preliminarmente si fornisce una sintetica descrizione dei reati contemplati nella presente Parte Speciale "E", coincidente con quelli indicati nell'articolo 25 undicies del Decreto.

- **condotte illecite nei confronti di specie animali e vegetali selvatiche protette (articolo 727 bis del Codice Penale)**

Questa ipotesi di reato si configura nel caso in cui qualcuno, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta, oppure distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie.

La norma punisce quelle condotte illecite che causano un grave danno alla conservazione di una specie selvatica protetta (vegetale o animale), causando la morte di un elevato numero di esemplari di tale specie o sottraendone un elevato numero dal loro habitat naturale.

Esempio: Un'azienda, attiva nel commercio all'ingrosso di animali, cattura o fa catturare, per immetterle sul mercato, un ingente numero di animali appartenenti ad una specie protetta, perché in via di estinzione.

- **distruzione e deterioramento di habitat all'interno di un sito protetto (articolo 733 bis del Codice Penale)**

L' ipotesi di reato si configura nei casi in cui, qualcuno, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione.

La norma punisce i comportamenti illeciti che danneggiano gli habitat naturali compresi nei siti protetti, compromettendone lo stato di conservazione

Esempio: un'azienda che si occupa di raccolta e smaltimento rifiuti, scarica rifiuti pericolosi all'interno di un parco naturale, causando l'inquinamento del terreno e delle acque.

- **reati relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione (Legge 7 febbraio 1992 nr. 150)**

La norma punisce importazione esportazione, trasporto, utilizzo, detenzione e commercio di specie protette, perché potrebbero essere minacciate da attività di commercio indiscriminato o perché pericolose per le specie autoctone dei paesi in cui potrebbero essere introdotte.

Esempio: una azienda importa e commercializza in Italia specie protette, senza le prescritte licenze di importazione ed utilizzo

- **scarichi di acque reflue industriali senza autorizzazione (articolo 137 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui qualcuno non osservi i divieti di scarico previsti dagli articoli 103 e 104 del Testo Unico Ambientale.

La norma punisce sia il mancato rispetto dei limiti per lo scarico in acque superficiali o in fognatura sia la mancata osservanza del divieto di scarico al suolo, nel sottosuolo o nelle acque sotterranee. Ai sensi del Testo Unico Ambientale, infatti, è sempre vietato scaricare direttamente al suolo, nel sottosuolo e nelle acque sotterranee. Deroghe a tale divieto sono ammesse solo in un certo numero di casi (individuati nel Testo Unico Ambientale). Al di fuori di tali casi, gli scarichi sul suolo devono essere convogliati in corpi idrici superficiali, in reti fognarie oppure destinati al riutilizzo in conformità alle prescrizioni di legge; mentre gli scarichi nel sottosuolo e nelle acque sotterranee, debitamente autorizzati, devono essere convogliati in corpi idrici superficiali oppure destinati, ove possibile, al riciclo, al riutilizzo o all'utilizzazione agronomica.

- **attività di gestione rifiuti non autorizzata (articolo 256 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui qualcuno effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione.

La norma intende sanzionare le attività abusive di raccolta, recupero, smaltimento, commercio, intermediazione dei rifiuti, vale a dire quelle attività che non dispongono delle autorizzazioni o delle iscrizioni previste dal Testo Unico Ambientale.

Esempio: un'azienda esercita la raccolta e il trasporto di rifiuti senza essere iscritta all'albo nazionale dei gestori ambientali

- **Mancata bonifica e mancata comunicazione di evento inquinante (articolo 257 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui qualcuno cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque

sotterranee con il superamento delle concentrazioni soglia di rischio è punito se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente.

La norma punisce coloro che, al verificarsi di un evento potenzialmente in grado di contaminare un sito, non provvedono a comunicare tale evento alle autorità competenti (al comune, alla provincia, alla regione, o alla provincia autonoma nel cui territorio si prospetta l'evento lesivo, nonché al Prefetto della provincia); affinché siano intraprese tutte le verifiche atte a determinare la possibile entità dell'evento inquinante;

Punisce inoltre coloro che non provvedono alla bonifica dei siti inquinati, in conformità al progetto approvato dalle autorità competenti.

Esempio: un'azienda omette di bonificare un sito inquinato a causa di un incidente avvenuto in uno dei suoi reparti produttivi.

- **violazione obblighi di comunicazione, tenuta dei registri obbligatori e dei formulari (articolo 258 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui qualcuno, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.

La norma punisce le imprese che, effettuando il trasporto dei propri rifiuti non pericolosi, falsificano i dati relativi alla natura, alla composizione o alle caratteristiche chimico-fisiche dei rifiuti.

Esempio: un'azienda trasporta in discarica i rifiuti non pericolosi prodotti nei suoi stabilimenti, falsificando il certificato relativo ai rifiuti trasportati

- **traffico illecito di rifiuti (articolo 259 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui qualcuno effettua una spedizione di rifiuti costituente traffico illecito.

La norma punisce il traffico illecito di rifiuti all'interno della Comunità Europea, nonché in entrata e in uscita dal suo territorio. Costituisce traffico illecito qualsiasi spedizione di rifiuti:

1. effettuata senza che la notifica sia stata inviata a tutte le autorità competenti interessate

2. effettuata senza il consenso delle autorità competenti interessate

3. effettuata con il consenso delle autorità competenti interessate ottenuto mediante falsificazioni, false dichiarazioni o frode

4. non concretamente specificata nel documento di accompagnamento

5. che comporti uno smaltimento o un ricupero in violazione delle norme comunitarie o internazionali.

Esempio: un'azienda spedisce rifiuti, senza il consenso delle autorità competenti

- **attività organizzate per traffico illecito di rifiuti (articolo 260 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui qualcuno, al fine di conseguire un ingiusto profitto, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti.

L'articolo definisce e sanziona le attività organizzate per il traffico illecito dei rifiuti, che sono caratterizzate da:

1. Continuità nel tempo

2. Allestimento di mezzi e di una organizzazione, finalizzati alla gestione abusiva dei rifiuti

3. Conseguimento di un ingiusto profitto, derivante dal traffico dei rifiuti

Esempio: un'azienda mette a disposizione i propri mezzi, per realizzare traffico illecito di rifiuti

- **installazione di impianto in assenza di autorizzazione (articolo 279 del Decreto Legge 3 aprile 2006 nr. 152)**

Tale ipotesi di reato si configura nel caso in cui il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

Il comma punisce chiunque, nell'esercizio di una attività, produce emissioni in atmosfera tali da causare il superamento dei valori limite di qualità dell'aria

Esempio: Per un guasto dovuto agli scarsi investimenti nella manutenzione degli impianti, uno stabilimento produce emissioni inquinanti, che causano il superamento dei valori limite della qualità dell'aria dell'area in cui è sita l'azienda

- **produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive dell'ozono stratosferico (Legge 28 dicembre 1993 nr. 549)**

La norma punisce chiunque impieghi sostanze dannose per l'ozono, al di fuori dei limiti stabiliti dalla legge

Esempio: cicli produttivi di un'azienda producono sostanze lesive dell'ozono.

- **inquinamento provocato da navi (Decreto Legge 6 novembre 2007 nr. 202)**

Tale ipotesi di reato si configura nel caso in cui vi sia lo scarico nelle acque del mare da parte di navi od aeromobili di sostanze o materiali per i quali è imposto il divieto assoluto di sversamento, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purchè in presenza di preventiva autorizzazione da parte dell'autorità competente.

Il comma punisce lo sversamento in mare non autorizzato, da parte di navi o aerei, di ingenti quantità di sostanze vietate ai sensi delle convenzioni internazionali vigenti in materia, ratificate dall'Italia.

Esempio: Una nave riversa in mare una ingente quantità di sostanze vietate dalle convenzioni internazionali vigenti, in materia di tutela dei mari.

6.2 Aree a Rischio

Tenuto conto dell'attività svolta dall'azienda in relazione a quanto sopra e compatibilmente con quanto già riportato nella Parte Generale del presente Modello, vengono considerate (ai fini della presente Parte Speciale, Allegato "E") le seguenti aree di attività rischio:

- Gestione delle pratiche amministrative relative allo smaltimento dei rifiuti e della selezione dei fornitori di trasporto rifiuti
- Gestione delle autorizzazione allo scarico
- gestione delle altre "attività sensibili".

L'integrazione delle suddette aree di attività a rischio potrà essere disposta dall'Organo Amministrativo, su eventuale indicazione dell'Organismo di Vigilanza, il quale individuerà le relative ipotesi e definirà gli opportuni provvedimenti operativi.

6.3 Principi e comportamenti per la prevenzione dei reati Ambientali

La presente Parte Speciale Allegato "E" prevede l'espresso divieto, a carico degli esponenti aziendali (amministratori, dirigenti, dipendenti), in via diretta, e a carico dei collaboratori esterni, in via contrattuale, di tenere le seguenti condotte:

1) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25 undicies del Decreto);

2) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

Oltre a quanto previsto e ribadito nel Codice Etico, nell'ambito dei suddetti comportamenti, si riportano di seguito alcune misure preventive:

- I processi aziendali devono essere condotti in modo tale da non ledere l'integrità dell'ambiente.

- I soggetti terzi, che si occupano del trasporto dei rifiuti prodotti dalla società, devono prendere visione, accettare ed attenersi al modello organizzativo, ai divieti e alle procedure della presente parte speciale, finalizzati ad impedire la commissione di reati ambientali.

- Le vasche di stoccaggio delle acque reflue devono essere sottoposte a costante verifica dell'integrità, per evitare il rilascio nell'ambiente di sostanze inquinanti. Un apposito registro delle verifiche e manutenzioni effettuate deve essere aggiornato a cura del Responsabile di funzione.

- Il Responsabile di funzione approva tutte le attività aziendali che possano avere un impatto ambientale, e vigila sul rispetto della vigente normativa, per prevenire il concretizzarsi di comportamenti illeciti

- Il Responsabile di funzione è delegato a partecipare alle ispezioni poste in essere a carico della società dalle Autorità competenti per la tutela dell'ambiente.

- Il Responsabile di funzione deve prestare la propria collaborazione all'autorità che sta svolgendo l'attività di verifica, astenendosi dal porre in atto comportamenti od omissioni che possono ostacolare il regolare esito dell'Ispezione.

- Al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito, il Responsabile di funzione informa tempestivamente l'Organismo di Vigilanza e mette in opera entro ventiquattro ore le misure necessarie di prevenzione. La medesima procedura si applica all'atto di

individuazione di contaminazioni storiche che possano ancora comportare rischi di aggravamento della situazione di contaminazione.

6.4 Protocolli operativi specifici per la prevenzione dei reati ambientali

L'analisi dei processi aziendali ha individuato le principali aree a rischio di reato sopra descritte.

Nell'ambito di un processo di revisione, il sistema organizzativo di controllo (CdA, Collegio Sindacale, Disposizioni Operative, Procure, Ordini di Servizio, Procedure Operative interne ecc. ecc.) ha consentito di individuare le seguenti regole:

- Nell'ambito della gestione delle pratiche amministrative relative allo smaltimento dei rifiuti deve essere tenuta una condotta conforme a quanto previsto nelle procedure aziendale IO.6.3-05, P6.3-01 e successive modifiche.

- Nell'ambito della gestione delle autorizzazioni allo scarico, deve essere tenuta una condotta conforme a quanto previsto nelle procedure aziendali P2.2-01 e M2.2-01

- gestione delle altre "attività sensibili".

6.5 Controlli dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organo di Vigilanza di attivarsi con specifici controlli, anche a seguito delle segnalazioni ricevute, in relazione all'osservanza del Modello i suo compiti per quanto concerne i reati sopra contemplati sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale
- valutare periodicamente l'efficacia del Modello e delle procedure atte a prevenire la commissione dei Reati in materia ambientale.
- proporre ai soggetti competenti della Società eventuali azioni migliorative;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

In ragione dell'attività di vigilanza attribuitagli, si garantisce all'Organismo di Vigilanza libero accesso a tutta la documentazione aziendale rilevante.

Il presente Modello organizzativo parte speciale è stato approvato dal CdA in data 08/02/2013.