IL MODELLO

DI ORGANIZZAZIONE

GESTIONE E CONTROLLO

PARTE SPECIALE

Documento approvato con delibera del Presidente del __/__/20__ rev.o

INDICE

PARTE SPECIALE: I PROTOCOLLI

PREMESSA

La violazione di quanto previsto nei protocolli, quale parte integrante del Modello, determina la possibilità di applicazione delle sanzioni disciplinari espressamente previste dal modello stesso per le ipotesi di sua violazione; salva, ovviamente, l'applicabilità anche di altre norme legislative e regolamentari vigenti. Ai seguenti protocolli si intendono richiamate, quali parte integranti degli stessi, le procedure previsti nel manuale di gestione qualità e del Sistema della Privacy adottato dalla Rossi Medardo s.p.a.

CAP. I : I REATI INFORMATICI

L'art.7 della legge n.48/2008, mediante l'inserimento nell'ambito del D.Lgs. 231/01 dell'art.24 bis sui delitti informatici e trattamento illecito dei dati di seguito riportati, ha introdotto nuove fattispecie di reato che possono generare una responsabilità in capo alla Società.

Nella presente parte speciale sono definiti i principi generali relativi alle attività sensibili nel campo informatico, al fine di prevenire i reati di cui all'art. 24bis del D.Lgs.231/01.

Per completezza d'informazione si sottolinea che non si può realisticamente escludere alcuna area aziendale dal rischio di commissione dei delitti in oggetto, nella misura in cui in essa si faccia uso di sistemi hardware, software e telematici.

1.1 LE FATTISPECIE DEI REATI INFORMATICI DI CUI ALL'ART. 24 BIS DEL D.LGS. 231/2001

Per quanto riguarda i reati contemplati dall'art. 24 bis del Decreto riferibili all'attività della Rossi Medardo s.p.a. si provvede di seguito a fornire una breve descrizione:

1.1.1.ART. 24 BIS COMMA 1 D.LGS. 231/2001

Gli articoli del Codice Penale, previsti nel comma 1 dell'articolo 24 bis del D.Lgs.231/01, hanno come fattore comune il "danneggiamento informatico"; si parla di danneggiamento informatico quando considerando la componente hardware e software interviene una modifica tale da impedire il funzionamento, anche solo parziale.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (art. 615 ter c.p.)

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

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita

anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema:

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

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

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa;negli altri casi si procede d'ufficio."

La norma non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "*ius excludendi alios*", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati sia che titolare dello "*ius excludendi*" sia persona fisica, sia giuridica, privata o pubblica, o altro ente.

Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema, essendo reato di mera condotta, può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, mediante l'utilizzo di credenziali di altri colleghi abilitati.

Es. : Accesso abusivo nel sistema informatico di un concorrente al fine di conoscere il portafoglio clienti.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (art. 617-quater)

"Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrente tra più sistemi, ovvero impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisce 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 al primo e al secondo comma 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."

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software(cd. Spyware). L'impedimento o l'interruzione delle comunicazioni può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l' immissione di numerosissime comunicazioni fasulle.

Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall'installazione non autorizzata di un software da parte di un dipendente.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (art. 635 bis c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella,altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se ricorre la circostanza di cui al 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 a quattro anni e si procede d'ufficio".

Secondo un'interpretazione rigorosa, nel concetto di" programmi altrui" si ricomprendono anche i programmi utilizzati dal soggetto agente in quanto a lui già concessi in licenza dai legittimi titolari.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (art. 635 quater c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'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) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con l'abuso della qualità di operatore del sistema , la pena è aumentata.

E' da ritenere che la fattispecie di danneggiamento di sistema assorba le condotte di danneggiamento dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento.

Qualora la condotta descritta dal presente articolo consegua ad un accesso abusivo del sistema, essa sarà punita ai sensi dell'articolo 615 ter c.p.

D.LGS. N. 196/2003 E S.M.I. CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI. ART. 23 - CONSENSO

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

ART. 26 - GARANZIE PER I DATI SENSIBILI

I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.

Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

Il comma 1 non si applica al trattamento:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria;

b-bis) dei dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis. (36)

I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

I dati idonei a rivelare lo stato di salute non possono essere diffusi.

PARTE III, TITOLO III, CAPO II "ILLECITI PENALI"

ART. 167 - TRATTAMENTO ILLECITO DI DATI

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

ART. 169 - MISURE DI SICUREZZA

Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione

amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23, e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

1.1.2.ART. 24 BIS COMMA 2 D.LGS. 231/2001

Gli articoli del Codice Penale previsti nel comma 2 dell'art. 24 bis D.Lgs. 231/2001, hanno come fattore comune la detenzione o diffusione di codici o programmi atti al danneggiamento informatico. Da un punto di vista tecnico, gli artt. 615quater e 615 quinquies possono essere considerati accessori ai precedenti artt. 615ter, 635bis, 635ter e 635quater: la detenzione o dissezione di codici di accesso o la detenzione o diffusione di programmi o dispositivi diretti a danneggiare o interrompere un sistema telematico, di per sé non compiono alcun danneggiamento, se non utilizzati per un accesso abusivo ad u sistema o nella gestione di un'intercettazione di informazioni.

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615 QUATER C.P.)

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo,è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

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

Tale fattispecie intende reprimere la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici, rispetto ai quali le condotte in parola possono risultare propedeutiche.

DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (ART. 615 QUINQUIES C.P.)

"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso a da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale,o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni con la multa sino ad euro 10.329"

Nella valutazione della condotta criminosa assume preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e-mail, da parte di chi, pure non essendo mosso da specifica finalità di lucro o di determinazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

1.1.3. ART. 24 BIS COMMA 3 D.LGS. 231/2001

FALSITA' DI DOCUMENTI INFORMATICI (ART.491 BIS C.P.)

"Se alcune delle ipotesi previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".

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 specificatamente destinati ad elaborarli.

Tipologie delittuose rilevanti, a mero titolo esemplificativo, sono: falsità materiali commesse da un pubblico ufficiale o da un incaricato di un pubblico esercizio in atti pubblici e documenti ad essi assimilabili; falsità materiali in scrittura privata; falsità ideologiche in documenti pubblici commesse da un pubblico ufficiale, da incaricato di pubblico servizio ovvero da un privato; uso di atto falso (qualora l'autore materiale del reato non sia precedentemente concorso nella falsificazione del documento); soppressione, distruzione e occultamento, parziale o totale, di atti .

1.2.ELEMENTI ESSENZIALI DELLE PROCEDURE PER LA FORMAZIONE E L'ATTUAZIONE DELLE DECISIONI RELATIVE ALLE OPERAZIONI A RISCHI

1.2.1. INDIVIDUAZIONE DEL RESPONSABILE INTERNO

Per garantire un utilizzo e una gestione lecita e sicura del sistema informatico, i dovrà provvedere alla nomina di un soggetto (c.d. Responsabile Interno, che può coincidere con il Responsabile del Trattamento), al quale sarà attribuita la funzione di responsabile delle attività informatiche e telematiche considerate potenziali a rischio di reato.

In particolare, il Responsabile Interno deve;

- attuare i controlli preventivi previsti nella presente parte speciale, in della Rossi Medardo s.p.a., la protezione della rete da intrusioni di virus e la protezione del materiale informatico da utilizzi impropri;
- comunicare, attraverso la redazione di *report* informativi, all'Organismo di Vigilanza qualunque anomalia o criticità riscontrata nel corso dello svolgimento dell'attività nell'ambito della funzione di competenza;
- impartire a tutti i dipendenti e collaboratori adeguata formazione tecnica sull'utilizzo della strumentazione informatica e sulle regole comportamentali e procedurali a cui si devono attenere.

1.2.2.PRINCIPI GENERALI DI COMPORTAMENTO

Tutti i dipendenti della Rossi Medardo s.p.a. destinatari del Modello si devono attenere a principi di ordine generale al fine di prevenire, ed impedire, il verificarsi degli illeciti in materia informatica e di trattamento illecito dei dati.

In particolare essi:

- si astengono dalla falsificazione di qualsiasi documento informatico;

- si astengono dall'effettuare accessi abusivi a sistemi informatici o telematici e dal detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici;
- non usano né diffondono apparecchiature, dispositivi o programmi informatici che possano in qualsiasi modo danneggiare o interrompere un sistema informatico o telematico;
- si astengono dall'intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche e dall'installare apparecchiature idonee ad intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- non effettuano alcuna attività rivolta la danneggiamento di informazioni, dati e programmi informatici o al danneggiamento di sistemi informatici e telematici;
- si attengono scrupolosamente alle istruzioni operative e alle procedure aziendali diffuse e in uso presso la Rossi Medardo s.p.a.

Ulteriori regole di condotta di portata più specifica devono poi essere osservate da tutti i dipendenti della Società che hanno accesso e che utilizzano il sistema informatico, ai quali viene assegnato un computer, portatile o fisso (di proprietà della medesima), al solo scopo di eseguire attività inerente alle mansioni esercitate.

A tutti i destinatari del Modello è vietato:

- utilizzare il computer a propria disposizione per scopi esclusivamente personali;
- eseguire o tentare di eseguire installazioni di prodotti software in proprio possesso senza l'autorizzazione del Responsabile Interno;
- consentire a soggetti, interni od esterni alla Società, di accedere al proprio computer anche temporaneamente;
- inserire nel computer alcun supporto di memorizzazione esterno, tipo dischi fissi esterni, chiavette usb, dvd o cd, qualora i medesimi supporti non siano di provenienza conosciuta e garantita;
- collegare il computer aziendale a reti informatiche di cui non si conoscono i dettagli e comunque senza l' autorizzazione del Responsabile Interno;
- salvare dati al di fuori del proprio profilo utente in modo che siano visibili da altri che si collegano al computer con un altro identificativo;
- copiare dati aziendali sui computer personali o su dispositivi rimovibili, qualora non sia strettamente necessario per fini lavorativi;
- inviare per posta elettronica dati sensibili;
- configurare l'accesso remoto su computer diversi da quello in uso;
- consentire a chiunque esterno all'azienda di collegare il proprio computer alla rete aziendale;
- installare software contraffatti.

1.3.PROTOCOLLI DI CONTROLLO

Tutti i destinatari del Modello, adottano regole di condotta conformi:

- ai principi contenuti nel Codice Etico (che si intende integralmente richiamato), che costituiscono presupposto e parte integrante dei protocolli di prevenzione di seguito riportati;
- ai principi generali di comportamento precedentemente illustrati;
- i protocolli specifici di seguito rappresentati;
- sistema di Gestione della dati- privacy.

1) OBBLIGO DI INVENTARIO

Il responsabile Interno verifica almeno annualmente l'esatta consistenza del materiale informatico presente in Rossi Medardo s.p.a., evidenziando in particolare la presenza di:

-computer;
- software applicativo legato all'hardware;
- software applicativo di servizio aziendale;
- connessioni internet;
- server;
- contratti di licenza di programmi informatici;
- account di posta elettronica;
- altri supporti informatici;
- siti web

Il Responsabile Interno redige e aggiorna un documento nel quale, oltre alla descrizione del materiale informatico presente in azienda, indica per ciascun dipendente le dotazioni rispettivamente assegnate.

2) PROTEZIONE DELLA RETE DA INTRUSIONI INFORMATICHE, VIRUS, ETC.

Il Responsabile Interno garantisce la protezione della rete informatica con misure tecnologicamente adeguate. In particolare cura che:

- tutti i computer aziendali (fissi e portatili) ed il server siano dotati di sistemi antivirus, firewall e protezioni da eventuali aggressioni esterne;
- i sistemi antivirus siano quotidianamente aggiornati secondo un programma di upgrade aggiornato;
- ogni supporto che venga installato e/o utilizzato su computer aziendali sia preventivamente sottoposto a scansione antivirus.
- sia effettuato il controllo dell'integrità del backup quotidiano e almeno una volta al mese si effettui il test di recovery;

3) PROTEZIONE DEL MATERIALE INFORMATICO DA UTILIZZI IMPROPRI

Il Responsabile Interno cura che tutti i computer siano dotati di username personale riferibile al singolo utente, nonché di una password di protezione che deve essere inserita dall'utilizzatore e comunicata esclusivamente al R.I.

I computers aziendali devono essere impostati in modo che durante la fase di standby l'utilizzo divenga possibile solo previo inserimento della password, che devono essere periodicamente modificate.

E' vietato ogni accesso non autorizzato al server aziendale, con particolare riguardo alle applicazioni gestionali e di condivisioni delle informazioni.

4) UTILIZZO DELLA POSTA ELETTRONICA

Ogni dipendente o collaboratore della Rossi Medardo s.p.a. ha assegnato un indirizzo di posta elettronica personale sul dominio della Società.

L'accesso all'indirizzo di posta elettronica è riservato esclusivamente al titolare e, a tal fine, ogni account viene protetto da password inserita dallo stesso e comunicata al R.I.

È fatto divieto di utilizzare indirizzi di posta elettronica diversi, salvo che ciò non sia giustificato da motivi tecnici e purché vi sia preventiva autorizzazione da parte del titolare.

L'account di posta elettronica deve essere utilizzato esclusivamente per ragioni connesse con l'attività lavorativa.

E' fatto divieto inviare contenuti informativi aziendali anche parziali attraverso qualsiasi account di posta elettronica.

5) PROGRAMMI INSTALLATI SU COMPUTERS AZIENDALI

E' fatto divieto di installare qualsiasi programma da parte dell'utente o di altri operatori non autorizzato.

6) FORMAZIONE DEI DIPENDENTI

Il Responsabile Interno cura che sia impartita a tutti i dipendenti e collaboratori della Rossi Medardo s.p.a. adeguata formazione tecnica sull'utilizzazione della strumentazione informatica e sulle regole comportamentali procedurali a cui si devono attenere.

A tal fine il R.I. cura che tutti i dipendenti e i collaboratori abbiano conoscenza delle istruzioni operative adottate dalla Società in merito all'utilizzo di sistemi informatici, nonché dei presenti Protocolli.

1.4 OBBLIGHI DI COMUNICAZIONE ALL'ODV

Ciascun utente è tenuto a segnalare all'R.I. ogni violazione, tentativo o sospetto di violazione, nonché qualsiasi malfunzionamento del sistema informatico.

Il R.I. effettua i controlli nelle aree a rischio individuate e segnala tempestivamente all'Odv qualsiasi anomalia dovesse riscontrare e ogni modifica apportata al regolamento aziendale sull'utilizzo dei sistemi informativi.

La rete informatica aziendale è periodicamente sottoposta ad attività di controllo, amministrazione e back – up finalizzate alla rimozione di ogni file o applicazione ritenuti pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui PC dei lavoratori, sia sulle rete aziendale.

Il Responsabile segnala altresì periodicamente la necessità di sottoporre l'intero sistema informatico aziendale a check-up da parte di società specializzate.

CAP. II : I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Nella presente Parte Speciale sono definiti i principi generali di riferimento relativi alle Attività Sensibili individuate nei rapporti con la Pubblica Amministrazione, al fine di prevenire i reati di cui all'artt.24 e 25 del D. lgs. 231/2001. Nelle pagine che seguono verranno individuate:

- le fattispecie dei reati nei rapporti con la Pubblica Amministrazione di cui all' 24 e 25 del D.lgs. 231/2001 riferibili all'attività della Rossi Medardo s.p.a.;
- i destinatari del presente protocollo e i principi generali di comportamento;
- la definizione delle procedure per la prevenzione dei reati contro la P.A.;
- procedure aziendali specifiche.

2.1 LE FATTISPECIE DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE DI CUI ALL'ART. 24 DEL D.LGS. 231/2001

ART. 640, COMMA 2, N. 1, C.P. TRUFFA COMMESSA A DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e con la multa da € 51 a € 1.032.

La pena è della reclusione da 1 a 5 anni e della multa da € 309 a € 1.549 se il fatto è commesso a danno dello Stato o di altro ente pubblico.

Lo schema di questo reato è quello tradizionale della truffa (induzione in errore del soggetto attraverso una difforme rappresentazione della realtà, con ottenimento di un indebito beneficio e danno altrui) e si caratterizza per il soggetto raggirato: lo Stato o un altro Ente Pubblico.
Area a rischio di reato rilevante in Rossi Medardo s.p.a. è la partecipazione a gare e/o appalti pubblici.

2.2 LE FATTISPECIE DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE DI CUI ALL'ART. 24 DEL D.LGS. 231/2001

Si considerano rilevanti nel contesto della Rossi Medardo s.p.a. le seguenti fattispecie, in quanto il rischio viene considerato medio.

ART. 318 C.P. CORRUZIONE PER UN ATTO D'UFFICIO

Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a tre anni.

Se il pubblico ufficiale riceve la retribuzione per un alto d'ufficio da lui già compiuto, la pena è della reclusione fino a un anno.

Il reato in esame può essere commesso, oltre che dal p.u., anche dall'incaricato di un pubblico servizio "qualora rivesta la qualità di pubblico impiegato" (art. 320 c.p.).

Rispetto alla concussione, la corruzione sia propria (art. 319 c.p.) che impropria (art. 318 c.p.) si caratterizza per l'accordo illecito raggiunto tra i diversi soggetti.

Questa fattispecie si caratterizza per il rapporto paritetico che intercorre tra il soggetto pubblico e il privato corruttore. Nell'ipotesi ora esaminata (corruzione impropria), il pubblico ufficiale o l'incaricato di un pubblico servizio si accorda con il dipendente per compiere un atto comunque del suo ufficio. Tale deve intendersi qualunque atto che costituisca concreto esercizio di poteri inerenti all'ufficio di appartenenza del funzionario.

La differenza tra questa ipotesi di corruzione (impropria) e quella successiva "per atto contrario ai doveri d'ufficio" art. 319 c.p. si ravvisa nel fatto che, nel primo caso, si realizza (a seguito dell'accordo con il privato) da parte del pubblico ufficiale una violazione del principio di correttezza e, in qualche modo, del dovere di imparzialità, senza tuttavia che la parzialità si trasferisca nell'atto. Nel secondo caso, la parzialità colpisce l'atto che non realizza la finalità pubblica ad esso sottesa e viene compiuto ad uso privato.

ART. 319 C.P. CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO

Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da due a cinque anni.

Il privato corruttore nella corruzione "propria" si assicura con la promessa o la dazione indebita un atto del pubblico ufficiale che contrasta con i doveri del suo ufficio.

Per stabilire se un atto sia contrario o meno ai doveri d'ufficio occorre avere riguardo non soltanto all'atto in sé per verificarne la legittimità o l'illegittimità ma anche alla sua conformità a tutti i doveri d'ufficio o di servizio che possono venire in considerazione, con il risultato che un atto può essere in se stesso non illegittimo e ciò nondimeno essere contrario ai doveri d'ufficio. La verifica deve essere fatta non in relazione a singoli atti, ma tenendo presente l'insieme del servizio reso al privato.

ART. 322 C.P. ISTIGAZIONE ALLA CORRUZIONE

Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, per indurlo a compiere un atto del suo ufficio, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo.

Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.

La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 318.

La pena di cui al secondo comma su applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

Il delitto in esame si configura come reato di mera condotta. E' sufficiente per l'integrazione del reato la semplice offerta o promessa, purché sia caratterizzata da adeguata serietà e sia in grado di turbare psicologicamente il p.u. o l'incaricato di pubblico servizio così da far sorgere il pericolo che lo stesso accetti l'offerta o la promessa.

2.3 ATTIVITÀ SENSIBILI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

La Società, attraverso un'analisi effettuata, ha individuato alcuni Processi Sensibili le cui attività sono state analizzate e, dove ritenuto necessario, integrate con nuovi protocolli di controllo, che a loro volta risultano in costante e continuo aggiornamento.

I Processi Sensibili individuati si riferiscono principalmente a:

1. Gestione gare ed appalti pubblici;
2. Gestione dei rapporti con la Pubblica Amministrazione in caso di verifiche ed accertamenti;
3. Gestione approvvigionamenti e contratti di consulenze.

Tutti i Processi Sensibili devono essere svolti conformandosi alle leggi vigenti, ai valori e alle politiche della Rossi Medardo s.p.a., alle regole contenute nel Modello Organizzativo, nel Codice Etico e nei protocolli attuativi dello stesso.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

I divieti di carattere generale si applicano sia ai dipendenti e ai componenti degli Organi Sociali di Rossi Medardo s.p.a.. - in via diretta -, sia ai Consulenti e ai Fornitori, in forza di apposite clausole contrattuali. Nello specifico, è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati,

integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra indicate (artt. 24 e 25 D.Lgs. 231/2001).

E' fatto divieto in particolare di:

- accordare vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della Pubblica che possano determinare le stesse conseguenze previste al precedente punto;
- intervenire su sistemi informatici della Pubblica Amministrazione alterandone in qualsiasi modo il funzionamento.

Relativamente ai processi sensibili di carattere rilevante, occorre individuare, attribuendo alle stesse debita evidenza, adeguate procedure che garantiscano tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'O.D.V. tutta la documentazione di supporto.

2.4. I PRINCIPI GENERALI DI COMPORTAMENTO

Al fine di prevenire la commissione dei reati esaminati nella presente sezione, ai Destinatari è fatto esplicito divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino, individualmente o collettivamente, direttamente o indirettamente, una o più delle fattispecie di reato sopra considerate o che comunque agevolino la commissione dei predetti reati. Essi, in particolare, nell'ambito delle proprie funzioni, sono tenuti a rispettare le procedure aziendali previste dalla presente sezione e ad osservare la normativa in materia di reati contro la Pubblica Amministrazione.

Sono obbligati al rispetto dei seguenti principi generali:

- garantire la stretta osservanza di tutte le leggi e regolamenti vigenti che disciplinano l'attività aziendale, specie per quanto attiene ai rapporti tra la Rossi Medardo s.p.a. e la Pubblica Amministrazione;
- i rapporti con la Pubblica Amministrazione devono essere gestiti solo dalla funzione aziendale competente o dalle persone specificatamente autorizzate;
- la gestione dei rapporti con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio devono ispirarsi a criteri di correttezza e trasparenza, in modo da garantire il buon andamento della funzione o del servizio e, quindi, l'imparzialità nello svolgimento degli stessi.
- nei rapporti con lo Stato e con gli altri Enti pubblici, o comunque incaricati di pubblici servizi, la Società si impegna a fornire documentazione, dichiarazioni, certificazioni e informazioni corrette;

- la Società proibisce qualunque comportamento che può dare luogo a forme di corruzione e si impegna ad agire nel pieno rispetto della normativa vigente.

In particolare, le procedure specifiche previste dalla presente Parte Speciale precisano che è vietato:

1) effettuare o promettere elargizioni in denaro alla P.A. e quindi a pubblici funzionari o incaricati di un pubblico servizio;

2) distribuire omaggi e regali fuori dalla prassi aziendale specie se a pubblici funzionari o a loro familiari, tali che possono influenzare l'indipendenza del giudizio od indurre un qualsivoglia vantaggio per l'azienda. I regali offerti, salvo quelli di modico valore, debbono essere documentati, per effettuare le eventuali verifiche;

3) accordare altri vantaggi di qualsiasi natura, in favore di rappresentanti della P.A., che possano portare alle stesse conseguenze di cui al punto precedente;

4) riconoscere favori in compenso a professionisti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico e alla prassi vigente;

Nell'attuazione dei comportamenti di cui sopra:

1) i comportamenti con la P.A. devono essere gestiti in modo unitario, autorizzando in tal senso una persona responsabile per ogni operazione o pluralità di operazioni svolte nelle aree a rischio di reato;

2) gli incarichi conferiti ai professionisti esterni devono essere redatti per iscritto con l'indicazione dell'attività demandate e il relativo compenso;

3) nessun tipo di pagamento se non adeguatamente documentato può essere effettuato;

4) le dichiarazioni rese agli organismi pubblici devono contenere solo elementi assolutamente veritieri e per le eventuali somme ricevute deve essere rilasciato un apposito rendiconto.

2.5 ELEMENTI ESSENZIALI DELLE PROCEDURE PER LA FORMAZIONE E L'ATTUAZIONE DELLE DECISIONI RELATIVE ALLE OPERAZIONI A RISCHIO

2.5.1.INDIVIDUAZIONE DEL RESPONSABILE INTERNO

I rapporti con la Pubblica Amministrazione o con i terzi devono essere gestiti in modo unitario e di essi deve essere data debita evidenza. A tal fine il Presidente dovrà provvedere alla nomina di un soggetto (c.d. Responsabile Interno) responsabile per ogni singola operazione o pluralità di operazioni nell'ambito di quelle aree, ove più concreta è la possibilità di incorrere in una delle fattispecie di reato di cui agli artt. 24 e25 del D.lgs. 231/2001. Il Responsabile Interno dovrà a campione, mensilmente, verificare che siano effettivamente rispettate le procedure impartite ai lavoratori.

In particolare, il R.I. deve;

- segnalare all'Organo di Vigilanza, l'avvio dell'Attività Sensibile;
- comunicare, attraverso la redazione di report informativi, all'Organismo di Vigilanza qualunque anomalia o criticità riscontrata nel corso dello svolgimento dell'attività nell'ambito della funzione di competenza;
- verificare la concreta ed efficace attuazione, nell'ambito delle funzioni di competenza, delle procedure aziendali e dei principi di cui al presente Modello di organizzazione e gestione.

2.6 PROCEDURE AZIENDALI SPECIFICHE

2.6.1. PROCEDURE PER LA GESTIONE DEGLI ADEMPIMENTI IN MATERIA DI ISPEZIONI DA PARTE DI SOGGETTI PUBBLICI

Oltre agli adempimenti e agli obblighi imposti dalle normative vigenti in particolare dai D.lgs 81/2008 e D.lgs. 196/03, ai fini della prevenzione dei reati di cui all'art. 25 devono essere adottate procedure aziendali specifiche che individuino le modalità e le funzioni del Responsabile Interno nominato dal Presidente per la gestione dei rapporti, delle ispezioni e degli accertamenti, anche sui luoghi del lavoro, da parte di funzionari della Pubblica Amministrazione (quali ad esempio: funzionari degli enti locali, delle Aziende ASL, della DPL, del corpo della Guardia di Finanza etc.).

In particolare le procedure aziendali devono definire con chiarezza ruoli e competenze del Responsabile Interno nella gestione degli adempimenti in materia di ispezioni, di sicurezza dei luoghi di lavoro da parte di soggetti pubblici. E' suo onere:

- stabilire quando e come interpellare eventuali ulteriori funzioni o, in caso di necessità e di urgenza, le modalità per informare il Presidente;
- documentare mediante linee di reporting informativo l'attività svolta nel corso dell'ispezione, dai quali devono risultare i nominativi dei funzionari incontrati, i documenti richiesti e/o consegnati, i soggetti coinvolti nonché una relazione di sintesi delle informazioni verbali richieste e/o fornite;
- prevedere un rendiconto periodico sulla gestione degli adempimenti in materia di ispezioni da parte di soggetti pubblici da portare a conoscenza dell'Organismo di Vigilanza;
- denunciare direttamente all'Organismo di Vigilanza le anomalie riscontrate nel corso dell'attività di ispezione, fermo restando la responsabilità dell'ODV di riferire al

Presidente che sanzionerà tutti i comportamenti in contrasto con i principi di cui alla presente Parte Speciale.

Si richiama la procedura "norme di comportamento da adottare nel corso di un' ispezione o controllo".

2.6.2. GESTIONE APPROVVIGIONAMENTI E CONTRATTI DI CONSULENZA

Le relazioni con i fornitori sono regolate dai principi previsti nel presente Modello, dal manuale qualità, dalle procedure societarie e sono oggetto di costante monitoraggio. Le relazioni con i fornitori comprendono anche i contratti di consulenza. Si richiamano completamente le procedure previste nella qualità, ricordando che i contratti non possono essere negoziati, stipulati, e/o gestiti in autonomia da un solo soggetto. Eventuali successive integrazioni/modifiche del contratto devono essere adeguatamente controllate e autorizzate da un soggetto differente da quello che ha negoziato il contratto e l'atto formale della stipula del contratto deve avvenire esclusivamente in base al vigente sistema dei poteri e delle deleghe. I contratti devono contenere un'apposita dichiarazione con cui la controparte dichiara di essere a conoscenza e di impegnarsi nel rispetto del modello 231 e d ei relativi allegati, nonché una specifica clausola risolutiva espressa del contratto che preveda la risoluzione dello stesso ai sensi dell'art. 1456 c.c. e il diritto di Rossi Medardo s.p.a. al risarcimento del danno nel caso in cui l'impresa violi quanto previsto dal codice etico degli appalti, del modello 231 e il Codice Etico.

2.6.3. GESTIONE GARE E APPALTI PUBBLICI

La presente procedura ha lo scopo di definire le modalità adottate e le responsabilità coinvolte per la gestione delle attività di partecipazione ad appalti pubblici indetti dalla Pubblica Amministrazione.

Il Processo si riferisce alle attività finalizzate alla raccolta di informazioni, alla predisposizione e presentazione della documentazione per la partecipazione a gare ad evidenza pubblica e procedure negoziate, nonché alle attività legate alla gestione di tutte le fasi successive all'aggiudicazione.

Il processo di partecipazione a gare indette dalla PA è gestito e supervisionato dai Rappresentanti della Direzione sulla base della tipologia di bando e delle caratteristiche delle offerte richieste.

Principi specifici di comportamento e controllo

Oltre a quanto in generale, con riferimento al Processo Sensibile in oggetto devono essere rispettati i seguenti principi specifici di comportamento e controllo:

- tutti coloro che materialmente intrattengono rapporti con la Pubblica Amministrazione per conto della Società nell'ambito del processo di "negoziazione/stipula/esecuzione di contratti/convenzioni con soggetti pubblici nell'ambito di gare e/o nell'ambito di procedure negoziate" devono godere di un'autorizzazione in tal senso da parte della Società stessa, formalizzata, per quanto concerne dipendenti e gli organi sociali, in un'apposita procura o in una delega e direttive organizzative interne, ovvero in un contratto di fornitura/consulenza o di collaborazione per quanto concerne soggetti terzi che operano in nome, per conto o nell'interesse della Società;
- tutte le dichiarazioni e le comunicazioni rese a esponenti della Pubblica Amministrazione e previste dalle norme in vigore o specificatamente richieste dai suddetti esponenti in sede di incontri devono rispettare i principi di chiarezza, correttezza, completezza e trasparenza;
- il principio di segregazione dei compiti deve essere garantito dal coinvolgimento di soggetti differenti nello svolgimento delle principali attività previste dal processo (attività preliminari di partecipazione a bandi di gara, acquisizione delle informazioni relative al bando di gara, predisposizione della documentazione necessaria alla partecipazione alla fase di selezione/aggiudicazione, predisposizione dell'offerta tecnica e dell'offerta economica, inoltro della documentazione all'Ente Pubblico, gestione del riscontro da parte dell'Ente, stipula del contratto, gestione amministrativa del contratto, archiviazione della documentazione);

- è responsabilità dell'Ufficio Amministrativo che la Rossi Medardo s.p.a. sia in possesso di tutti i requisiti di tipo giuridico, economico ed organizzativo richiesti nel bando o nella Richiesta di Offerta;
- a seguito del formale invito a partecipare ad una gara, l'Ufficio approvvigionamento ha la responsabilità di predisporre, l'offerta finale. In particolare:

– è di competenza del Responsabile dell'Ufficio approvvigionamento l'invio documentazione raccolta utile alla partecipazione al bando, solo a seguito della verifica e controllo della da parte dell'Ufficio Amministrativo:

1. conformità dell'offerta con il capitolato di gara;
2. conformità degli aspetti amministrativi;
3. conformità degli aspetti economici;

- nel caso l'Azienda risulti aggiudicataria della gara, deve essere prevista la sottoscrizione del relativo contratto che deve essere sottoscritto dal rappresentante Legale della Società oppure dai soggetti muniti di procura
- il coinvolgimento nel processo di soggetti terzi deve essere regolato dalla predisposizione di un contratto formale;
-

2.7. CONTROLLI DELL'O.D.V.

L'O.d.V. effettua in piena autonomia specifici controlli e, periodicamente, controlli a campione sulle attività connesse ai Processi Sensibili, diretti a verificare la corretta implementazione delle stesse in relazione alle regole di cui al Modello Organizzativo.

A tal fine, all'O.D.V. viene garantito libero accesso a tutta la documentazione aziendale rilevante.

CAP. III : I REATI SOCIETARI

Nella presente Parte Speciale sono definiti i principi generali di riferimento relativi alle Attività Sensibili individuate nei rapporti societari, al fine di prevenire i reati di cui agli art. 25-ter del D. lgs. 231/2001.

Nelle pagine che seguono verranno individuate:

- la fattispecie di reato societario di cui agli art. 25-ter del D. lgs. 231/2001 riferibile all'attività della Rossi Medardo s.p.a.;
- i destinatari del presente protocollo e i principi generali di comportamento;
- la definizione delle procedure per la prevenzione dei reati societari.
- procedure aziendali specifiche.

3.1 LE FATTISPECIE DEI REATI NEI RAPPORTI SOCIETARI DI CUI ALL'ART. 25- TER DEL D.LGS. 231/2001

Per quanto riguarda i reati contemplati dall'art. 25- ter del Decreto riferibili all'attività della Rossi Medardo s.p.a. si provvede di seguito a fornire una breve descrizione:

FALSE COMUNICAZIONI SOCIALI (art. 2621 c.c.)

"Salvo quanto previsto dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.

Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa."

Il reato si configura quando l' amministratore, i direttori generali, i sindaci e i liquidatori di una società espongono, nei bilanci, nelle relazioni o in altre comunicazioni sociali previste dalla legge, dirette ai soci ed al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, oppure omettono, in modo idoneo ad indurre in errore i destinatari, informazioni la cui comunicazione è obbligatoria, sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene e quando la condotta in discorso è da essi tenuta con l'intenzione di ingannare i soci o il pubblico ed al fine di conseguire per sé o per altri un ingiusto profitto.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti od amministrati dalla società per conto terzi, mentre è esclusa se le falsità od omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene

La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5%, ovvero una variazione del patrimonio netto non superiore all'1%.

In ogni caso, il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10% da quella corretta.

Si noti che la fattispecie in esame è un *reato di pericolo* che si perfeziona con la semplice condotta descritta nella previsione normativa.

3.2 Le "attività sensibili relative ai reati societari" ai fini del d.lgs. 231/2001

L' attività sensibile individuata, in riferimento ai Reati Societari richiamati dall'art. 25-*ter* del d.lgs. 231/2001, è la seguente:

processo di predisposizione della bozza di bilancio e dei documenti collegati.

Esso è distinto nelle seguenti macro fasi:

1. gestione della contabilità generale;
2. definizione dei criteri di contabilizzazione delle poste di bilancio;
3. predisposizione e approvazione del bilancio di esercizio.

Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico dell'Assemblea dei Soci, del Presidente, del consulente esterno, del Responsabile Amministrativo della Rossi Medardo s.p.a. di :

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

La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei soggetti sopra indicati di rispettare scrupolosamente tutte le leggi vigenti ed in particolare di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio.

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

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;

b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società.

3.3 Principi generali di controllo

I principi contenuti nel Codice Etico (che qui si intende integralmente richiamato),costituiscono presupposto e parte integrante del protocollo di prevenzione previsto per la predisposizione e approvazione del bilancio di esercizio.

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare il presidio specifico di controllo possono essere sintetizzati come segue:

- **Segregazione delle attività**: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Esistenza di procedure/norme/circolari**: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma**: i poteri autorizzativi e di firma devono essere chiaramente definiti e conosciuti all'interno della Società.
- **Tracciabilità**: ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata.

Il processo di decisione, autorizzazione e svolgimento dell'Attività Sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

3.4 Protocollo per la predisposizione e approvazione del bilancio di esercizio

Il processo in oggetto è regolamentato dalle procedure amministrativo-contabili previste dal Codice Civile e dalla legislazione in materia. Il processo di predisposizione del bilancio e dei documenti collegati è distinto nelle seguenti macro fasi:

1. gestione della contabilità generale;
2. definizione dei criteri di contabilizzazione delle poste di bilancio;
3. predisposizione e approvazione del bilancio di esercizio

Nell'ambito del processo sono definiti ruoli, responsabilità ed attività di controllo, in particolare con riferimento alle sue diverse fasi.

1. il Presidente definisce le procedure di gestione contabile, il responsabile amministrativo e il consulente esterno le regole di contabilizzazione per la contabilità generale e analitica. Le scritture e le registrazioni contabili vengono effettuate in modo da riflettere accuratamente e correttamente tutte le operazioni della società. Tutti i costi e gli oneri, i ricavi e i proventi, gli incassi e gli esborsi sono rappresentati in contabilità in modo veritiero e corretto e opportunamente documentati in conformità alla legislazione vigente. La rilevazione delle informazioni contabili avviene tramite sistema informatico, a garanzia della tracciabilità dei singoli passaggi del processo di formazione dei dati. I profili di accesso a tali sistemi sono chiaramente identificati dal Responsabile Amministrativo e garantiscono la separazione dei compiti e la coerenza dei livelli autorizzativi.

2. La fase di definizione dei criteri di **contabilizzazione delle poste di bilancio** viene effettuata in base ai principi contabili previsti ex lege e si articola nelle seguenti attività:

- predisposizione dell'annotazione dei ricavi e dei costi;
- verifica, da parte del Consulente Esterno, delle metodologie di rappresentazione contabile delle poste di bilancio e del loro andamento;
- autorizzazione alla registrazione delle singole voci in contabilità generale, dopo aver acquisito ed analizzato, anche mediante l'intervento operativo dell'apposito consulente esterno, la relativa documentazione di supporto;
- registrazione in contabilità delle fatture attive e passive da parte del Responsabile Amministrativo ed archiviazione della documentazione di supporto presso l'ufficio di Contabilità.

3. fase di **predisposizione e approvazione del bilancio civilistico** può essere suddivisa in:

- predisposizione e diffusione del calendario di chiusura: il Presidente stabilisce un calendario di chiusura e predispone una check list ove individua le attività da svolgere, i responsabili e le scadenze prefissate per la redazione e l'approvazione della Proposta di Bilancio di esercizio;
- predisposizione della Proposta di Bilancio : il Responsabile Amministrativo, sulla base dei dati contabili di chiusura, predispone la bozza di Proposta di Bilancio di esercizio. Il Presidente provvede a verificare tale proposta, nel caso in cui ravvisi la necessità di effettuare delle correzioni o rettifiche vi provvede attraverso il

consulente esterno (commercialista). Inoltre, il Presidente coordina la predisposizione della relazione sulla gestione e della nota integrativa;

- approvazione della Proposta di Bilancio di esercizio: il Presidente dopo aver controllato e analizzato la Proposta di Bilancio di esercizio la sottopone all'attenzione dell'Assemblea dei Soci per la delibera.

CAP. IV : REATI IN VIOLAZIONE DELLE NORME RELATIVE ALLA TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LAVORO

Le fattispecie riguardano i reati di omicidio colposo (art. 589 c.p.) e di lesioni personali colpose gravi o gravissime (art. 590 c.p.) commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Per "norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro" si intendono non solo le norme inserite nelle leggi specificatamente antinfortunistiche, ma anche tutte quelle che, direttamente o indirettamente perseguono il fine di evitare incidenti sul lavoro o malattie professionali e che in genere tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui esso deve svolgersi.

Si intende completamente richiamato il sistema di gestione della sicurezza adottato dalla Società, contestualmente al Modello 231.