

MODELLO DI ORGANIZZAZIONE E GESTIONE

Ai sensi del Decreto Legislativo
8 giugno 2001, n. 231

S.I.S.S.I. Srl

SERVIZI INTEGRATI PER LA SALUTE, LA SICUREZZA E L'IMPIANTISTICA

VIA SAN FERELO 24
26900 LODI

Lodi, 11 MARZO 2011

S.I.S.S.I. s.r.l.

Servizi Integrati per la Salute, la Sicurezza e l'Impiantistica
Via S. Fereolo n° 24 - 26900 LODI
C.F. - P.I. 12009480158
E-Mail : info@sissisrl.it – Sito Internet : www.sissisrl.it

Il presente documento è di proprietà della ditta sopracitata e della **SISSI srl**. –
Sono vietate la riproduzione, anche
parziale, del contenuto del documento e della metodologia di valutazione adottata,
proprietà esclusiva di **SISSI srl**.
I trasgressori verranno puniti a norma di legge.

Azienda con sistema Qualità UNI EN ISO 9001:2008 Certificato da:



Certificato N.:18147-2007-AQ-MIL-SINCERT

**AZIENDA ACCREDITATA DALLA REGIONE LOMBARDIA N. ISCRIZIONE 0181 DEL 01/08/2008 SEZIONE B
ALBO REGIONALE DEGLI OPERATORI ACCREDITATI PER I SERVIZI
DI ISTRUZIONE E FORMAZIONE PROFESSIONALE**

INDICE

PARTE GENERALE

1 LA RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI	Pagina 4
1.1 IL REGIME GIURIDICO DELLA RESPONSABILITA' AMMINISTRATIVA: IL D. Lgs. 8 giugno 2001, n. 231 E LA SUA EVOLUZIONE	
1.2 LA FATTISPECIE PREVISTA DALLA LEGGE E LE SANZIONI COMMINATE	
1.3 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO: LA SUA ADOZIONE	
1.4 LE LINEE GUIDA ELABORATE DA CONFINDUSTRIA	
1.5 EVOLUZIONE GIURISPRUDENZIALE	
2 L'ADOZIONE DEL MODELLO	Pagina 11
2.1 SISSI srl	
2.2 APPROCCIO METODOLOGICO AL MODELLO	
2.3 IL MODELLO E IL CODICE ETICO A CONFRONTO	
2.4 I DESTINATARI DEL MODELLO	
3 L'ORGANISMO DI VIGILANZA	Pagina 17
3.1 IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA INTERNO "OdV"	
3.2 FUNZIONI E POTERI	
3.3 REPORTING DELL'ORGANISMO DI VIGILANZA AGLI ORGANI SOCIETARI	
3.4 REPORTING: PRESCRIZIONI GENERALI E PRESCRIZIONI SPECIFICHE OBBLIGATORIE	
3.5 RACCOLTA, CONSERVAZIONE E ARCHIVIAZIONE DELLE INFORMAZIONI	
3.6 STATUTO DELL'ORGANISMO DI VIGILANZA	
3.7 REGOLAMENTO DELL'ORGANISMO DI VIGILANZA	
4 FORMAZIONE E DIFFUSIONE DEL MODELLO	Pagina 20
4.1 DIPENDENTI	
4.2 COLLABORATORI ESTERNI E PARTNER	
5 IL SISTEMA DISCIPLINARE	Pagina 21
5.1 PRINCIPI GENERALI	
5.2 MISURE NEI CONFRONTI DEI DIPENDENTI	
5.3 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI	
5.4 MISURE NEI CONFRONTI DI SOGGETTI ESTERNI: COLLABORATORI, CONSULENTI E ALTRI SOGGETTI TERZI	
5.5 SISTEMA DISCIPLINARE	

PARTE SPECIALE

INTRODUZIONE **Pagina 22**

6 REATI CONTRO LA PUBBLICA AMMINISTRAZIONE **Pagina 22**

- 6.1 LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25)
- 6.2 AREE DI ATTIVITA' A RISCHIO ("ATTIVITA' SENSIBILI")
- 6.3 DESTINATARI DELLA PARTE SPECIALE
- 6.4 PRINCIPI GENERALI DI COMPORTAMENTO
- 6.5 PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI PRESCRITTI
- 6.6 PROCEDURE DI PREVENZIONE

7 REATI SOCIETARI **Pagina 27**

- 7.1 LA TIPOLOGIA DEI REATI SOCIETARI (ART. 25 TER DEL DECRETO)
- 7.2 AREE DI ATTIVITA' A RISCHIO
- 7.3 DESTINATARI DELLA PARTE SPECIALE
- 7.4 PRINCIPI GENERALI DI COMPORTAMENTO
- 7.5 PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI PRESCRITTI
- 7.6 PROCEDURE DI PREVENZIONE

8 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI **Pagina 37**

- 8.1 LA FATTISPECIE DI REATO
- 8.2 AREE DI ATTIVITA' A RISCHIO
- 8.3 DESTINATARI DELLA PARTE SPECIALE
- 8.4 PRINCIPI GENERALI DI COMPORTAMENTO
- 8.5 PROCEDURE DI PREVENZIONE

9 REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME **Pagina 42**

- 9.1 LA FATTISPECIE DI REATO
- 9.2 AREE DI ATTIVITA' A RISCHIO
- 9.3 DESTINATARI DELLA PARTE SPECIALE
- 9.4 PRINCIPI GENERALI DI COMPORTAMENTO
- 9.5 PROCEDURE DI PREVENZIONE

10 REATI IN MATERIA DI VIOLAZIONE DEI DIRITTI D'AUTORE **Pagina 46**

- 10.1 LA FATTISPECIE DI REATO
- 10.2 AREE DI ATTIVITA' A RISCHIO
- 10.3 DESTINATARI DELLA PARTE SPECIALE
- 10.4 PRINCIPI GENERALI DI COMPORTAMENTO
- 10.5 PROCEDURE DI PREVENZIONE

11 ATTIVITA' STRUMENTALI ALLA COMMISSIONE DEI REATI **Pagina 48**

- 11.1 ATTIVITA' STRUMENTALI ALLA COMMISSIONE DEI REATI
- 11.2 PROCEDURE DI PREVENZIONE

La SISSI ha predisposto i seguenti documenti specifici:

STATUTO ORGANISMO DI VIGILANZA
REGOLAMENTO ORGANISMO DI VIGILANZA
CODICE ETICO

ALLEGATO 1 **Pagina 49**

ALLEGATO 2 **Pagina 50**

ALLEGATO 3 **Pagina 51**

ALLEGATO 4 **Pagina 52**

ALLEGATO 5 **Pagina 53**

TABELLA ACQUISTI DI BENI E SERVIZI **Pagina 54**

Parte Generale

1. La Responsabilità Amministrativa degli Enti: Cenni normativi

1.1 Il regime giuridico della responsabilità amministrativa: D.Lgs 8 giugno 2001, n. 231 e la sua evoluzione

Il D.Lgs 8 giugno 2001, n. 231 (qui di seguito, per brevità, il Decreto)¹, ha introdotto nell'ordinamento italiano una peculiare forma di responsabilità, nominalmente amministrativa, ma sostanzialmente a carattere afflittivo-penale, a carico di società, associazioni ed enti in genere per particolari reati commessi nel loro interesse o vantaggio da una persona fisica che ricopra al loro interno una posizione apicale o subordinata.

I presupposti applicativi della nuova normativa possono essere, in estrema sintesi, indicati come segue:

- a) l'inclusione dell'ente nel novero di quelli rispetto ai quali il Decreto trova applicazione;
- b) l'avvenuta commissione di un reato compreso tra quelli elencati dallo stesso decreto, nell'interesse o a vantaggio dell'Ente;
- c) l'essere autore del reato un soggetto investito di funzioni apicali o subordinate all'interno dell'Ente;
- d) la mancata adozione o attuazione da parte dell'Ente di un modello organizzativo idoneo a prevenire la commissione di reati del tipo di quello verificatosi;
- e) in alternativa al punto che precede, per il solo caso di reato commesso da parte di un soggetto apicale, anche il mancato affidamento di autonomi poteri di iniziativa e controllo ad un apposito organismo dell'Ente (o l'insufficiente vigilanza da parte di quest'ultimo) e l'elusione non fraudolenta da parte del soggetto apicale del modello di prevenzione adottato dall'Ente stesso.

1.2 La fattispecie prevista dalla Legge e le sanzioni comminate

La responsabilità scatta qualora sia stato commesso **un reato** che:

- a) risulti compreso tra quelli indicati dal decreto nell'apposito elenco (qui di seguito, per brevità, un reato);
- b) sia stato realizzato anche o esclusivamente **nell'interesse o a vantaggio dell'ente**, salvo che in quest'ultima ipotesi il reato sia stato commesso nell'interesse esclusivo del reo o di terzi;
- c) sia stato realizzato da una **persona fisica**:
 - i. **in posizione apicale** (ossia che esercita una funzione di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che esercita, anche di fatto, la gestione e il controllo dello stesso: qui di seguito, per brevità, Soggetto Apicale); ovvero
 - ii. **sottoposta alla direzione o alla vigilanza di un Soggetto Apicale** (qui di seguito, per brevità, Soggetto Subordinato).

¹ Il provvedimento in esame ("Disciplina delle responsabilità amministrative delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"), pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001, è stato emanato in attuazione alla delega al Governo di cui all'articolo 11 della legge 29 settembre 2000, n. 300. Quest'ultima trova il suo antecedente logico in tutta una serie di atti stipulati a livello internazionale, elaborati in base all'articolo K.3 del Trattato sull'Unione Europea: Convenzione sulla tutela degli interessi finanziari delle Comunità europee, stipulata a Bruxelles il 26 luglio 1995; suo primo Protocollo stipulato a Dublino il 27 settembre 1996; Protocollo concernente l'interpretazione in via pregiudiziale, da parte della Corte di Giustizia delle Comunità europee, di detta convenzione, con annessa dichiarazione stipulata a Bruxelles il 29 novembre 1996; nonché Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione stipulata a Bruxelles il 26 maggio 1997 e Convenzione OCSE sulla lotta alla corruzione dei pubblici ufficiali stranieri nelle operazioni economiche internazionali, con annesso, stipulata a Parigi il 17 dicembre 1997.

L'elenco dei reati

Per effetto delle successive modifiche apportate al Decreto risultano attualmente assoggettati all'applicazione di quest'ultimo i seguenti reati, in forma consumata e, relativamente ai soli delitti, anche semplicemente tentata:

Delitti contro la Pubblica Amministrazione

Malversazione ai danni dello Stato (art. 316-bis c.p.)
Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.)
Truffa a danno dello Stato o di altro ente pubblico (art. 640, comma 2 c.p.)
Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)
Concussione (art. 317 c.p.)
Corruzione per un atto d'ufficio (art. 318 c.p.)
Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)
Corruzione in atti giudiziari (art. 319-ter c.p.)

Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
Istigazione alla corruzione (art. 322 c.p.)
Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità europee e di Stati membri (art. 322-bis c.p.)

Delitti contro la fede pubblica

Falsificazione di monete (art. 453 c.p.)
Alterazione di monete (art. 454 c.p.)
Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
Spendita ed introduzione nello Stato di monete falsificate (art. 455 c.p.)
Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 461 c.p.)
Fabbricazione o detenzione di filigrana o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 464 c.p.)
Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)

Reati societari

False comunicazioni sociali (art. 2621 c.c.)
False comunicazioni sociali in danno dei soci o dei creditori (art. 2622 c.c.)
Falsità nelle relazioni o comunicazioni delle società di revisione (art. 2624 c.c.)
Impedito controllo (art. 2625 c.c.)
Indebita restituzione dei conferimenti (art. 2626 c.c.)
Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Formazione fittizia del capitale (2632 c.c.)
Indebita ripartizione dei beni sociali da parte dei liquidatori (2633 c.c.)
Illecita influenza sull'assemblea (art. 2636 c.c.)
Aggiotaggio (art. 2637 c.c.)
Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)
Omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.)

<p>Delitti contro la personalità individuale</p> <p>Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.) Tratta di persone (art. 601 c.p.) Alienazione o acquisto di schiavi (art. 602 c.p.) Prostituzione minorile (art. 600 ter c.p.) Pornografia minorile (art. 600 ter c.p.) Detenzione di materiale pornografico (art. 600 quater c.p.) Pornografia virtuale (art. 600 quater c.p.) Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.)</p>
<p>Delitti contro la persona</p> <p>Pratiche di mutilazione agli organi genitali femminili</p>
<p>Delitti informatici e trattamento illecito di dati</p> <p>Falsità in documento informatico pubblico o avente efficacia probatoria Accesso abusivo ad un sistema informatico o telematico Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche Danneggiamento di informazioni, dati e programmi informatici Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità Danneggiamento di sistemi informatici o telematici Danneggiamento di sistemi informatici o telematici di pubblica utilità Frode informatica del certificatore di firma elettronica</p>
<p>Delitti di terrorismo</p> <p>Delitti con finalità di terrorismo o di eversione dell'ordine democratico</p>
<p>Market Abuse</p> <p>Abuso di informazioni privilegiate (art. 184 TUF) Manipolazioni di mercato (art. 185 TUF)</p>
<p>Reati transnazionali</p> <p>Associazione per delinquere (art. 416 c.p.) Associazione di tipo mafioso (art. 416-bis c.p.) Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43) Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309) Disposizione contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5 del testo unico di cui al D.Lgs 25 luglio 1998, n. 286) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) Favoreggiamento personale (art. 378 c.p.)</p>

<p>Omicidio colposo e lesioni colpose gravi e gravissime</p> <p>Omicidio colposo (art. 589 c.p.) Lesioni colpose gravi e gravissime (art. 590, terzo comma, c.p.) Entrambi i delitti se commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della sicurezza sul lavoro.</p>
<p>Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita</p> <p>Ricettazione (art. 648 c.p.) Riciclaggio (art. 648-bis c.p.) Impiego di beni o di utilità di provenienza illecita (art. 648-ter c.p.)</p>
<p>Abbandono di rifiuti</p> <p>Abbandono e deposito incontrollati di rifiuti sul suolo e nel suolo Immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee L'art. 192 del D.Lgs 152/06 prevede che, se "la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica", la persona giuridica risponde in solido, secondo le previsioni del D.Lgs 231/01.</p>
<p>Delitti contro l'industria ed il commercio</p> <p>Turbata libertà dell'industria o del commercio. (art. 513 c.p.) Illecita concorrenza con minaccia o violenza. (art. 513-bis c.p.) Frodi contro le industrie nazionali. (art. 514 c.p.) Frode nell'esercizio del commercio. (art. 515 c.p.) Vendita di sostanze alimentari non genuine come genuine. (art. 516 c.p.) Vendita di prodotti industriali con segni mendaci (art. 517 c.p.) Fabricazione e commercio di beni realizzati usurpando titoli di proprietà industriale. (art. 517-ter c.p.) Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari. (art. 517-quater c.p.)</p>
<p>Delitti in materia di violazioni del diritto d'autore</p>
<p>Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria</p>
<p>Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.</p>

Gli elementi negativi di fattispecie

Pur quando siano stati integrati tutti gli elementi positivi di cui sopra, la responsabilità prevista dal decreto a carico dell'ente non scatta se il reato è stato commesso²:

- I) da un **Soggetto Apicale**, se l'ente prova che:
 - a. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, **un modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello verificatosi** (qui di seguito, per brevità, il Modello);
 - b. il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il loro aggiornamento è stato affidato a **un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo** (qui di seguito, per brevità, l'Organo di Vigilanza). Negli enti di piccole dimensioni tali compiti possono essere svolti direttamente dall'organo dirigente;

² In verità, in materia societaria, la formulazione adottata dal legislatore delegato (art. 3 D.Lgs 11 aprile 2002, n. 61) contiene una variante testuale rispetto a quanto previsto dalla Legge. Si prevede infatti la responsabilità dell'ente per i reati di cui sopra, "(...) se commessi nell'interesse della società, degli amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica". Non è chiaro se la formulazione adottata sia derogatoria rispetto a quella valida in generale o se essa sia imputabile ad un mero difetto di coordinamento con quest'ultima.

- c. le persone hanno commesso il reato eludendo **fraudolentemente** i modelli di organizzazione e di gestione
 - d. non vi è stata omessa o insufficiente vigilanza da parte dell'Organo di Vigilanza (di seguito anche OdV)
- II) da un **Soggetto Subordinato**, se il **Pubblico Ministero** non prova che la commissione del reato è stata resa possibile **dall'inosservanza degli obblighi di direzione o vigilanza**. In ogni caso è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un **Modello**.

Le sanzioni previste dal Decreto a carico dell'ente sono:

- a) la sanzione pecuniaria;
- b) le sanzioni interdittive;
- c) la pubblicazione della sentenza di condanna;
- d) la confisca.

Le sanzioni predette sono applicate al termine di un complesso procedimento su cui diffusamente *infra*. Quelle interdittive possono essere applicate anche in via cautelare, benché mai congiuntamente tra loro, su richiesta al Giudice da parte del Pubblico Ministero, quando ricorrono entrambe le seguenti condizioni:

- a) sussistono **gravi indizi** per ritenere la sussistenza delle responsabilità dell'ente a norma di decreto;
- b) vi sono fondati e specifici elementi che fanno ritenere concreto il **pericolo che vengano commessi illeciti della stessa indole** di quello per cui si procede.

Nel disporre le misure cautelari, il Giudice tiene conto della specifica idoneità di ciascuna in relazione alla natura e al grado delle esigenze cautelari da soddisfare in concreto, della necessaria proporzione tra l'entità del fatto e della sanzione che si ritiene possa essere applicata all'ente in via definitiva.

La sanzione pecuniaria

La sanzione pecuniaria consiste nel pagamento di una somma di denaro nella misura stabilita dal Decreto, comunque non inferiore a € 10.329 e non superiore a € 1.549.370, da determinarsi in concreto da parte del Giudice mediante un sistema di valutazione bifasico (c.d. sistema "per quote").

Le sanzioni interdittive

Le sanzioni interdittive consistono:

- a) nella interdizione dall'esercizio dell'attività³;
- b) nella sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) nel divieto, temporaneo o definitivo, di contrattare con la pubblica amministrazione⁴, salvo che per ottenere le prestazioni di un pubblico esercizio; nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli già concessi; nel divieto, temporaneo o definitivo, di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano, anche congiuntamente tra loro, **esclusivamente in relazione ai reati per i quali sono espressamente previste da Decreto**, quando ricorre almeno una delle seguenti condizioni:

- a) l'ente ha tratto dal reato un **profitto di rilevante entità** e il reato è stato commesso da un **Soggetto Apicale** ovvero da un **Soggetto Subordinato** quando, in quest'ultimo caso, la commissione del reato è stata determinata o agevolata da **gravi carenze organizzative**;
- b) in caso di **reiterazione degli illeciti**.

Quand'anche sussistano una o entrambe le precedenti condizioni le sanzioni interdittive pur tuttavia non si applicano se sussiste anche solo una delle seguenti circostanze:

³ Comporta la sospensione ovvero la revoca delle autorizzazioni, licenze o concessioni funzionali allo svolgimento dell'attività.

⁴ Anche limitatamente a determinati tipi di contratto o a determinate amministrazioni.

- a) l'autore del reato ha commesso il fatto nel **prevalente interesse proprio o di terzi** e **l'ente non ha ricavato vantaggio** o ne ha ricavato un vantaggio minimo, oppure
- b) il **danno patrimoniale** cagionato è **di particolare tenuità**, oppure
- c) prima della dichiarazione di apertura del dibattimento di primo grado concorrono tutte le seguenti condizioni:
 - 1. l'ente **ha risarcito integralmente** il danno e **ha eliminato le conseguenze dannose o pericolose del reato** ovvero si è comunque efficacemente adoperato in tale senso;
 - 2. l'ente **ha eliminato le carenze organizzative** che hanno determinato il reato mediante **l'adozione e l'attuazione di un Modello**;
 - 3. l'ente **ha messo a disposizione il profitto** conseguito ai fini della confisca.

La pubblicazione della sentenza di condanna

La pubblicazione della sentenza di condanna consiste nella pubblicazione di quest'ultima una sola volta, per estratto o per intero, a cura della cancelleria del Giudice, a spese dell'ente, in uno o più giornali indicati dallo stesso Giudice nella sentenza nonché mediante affissione nel comune ove l'ente ha la sede principale.

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

La confisca

La confisca consiste nell'acquisizione coattiva da parte dello Stato del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti in ogni caso salvi i diritti acquisiti dai terzi in buona fede; quando non è possibile eseguire la confisca in natura, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

1.3 Il Modello di Organizzazione, Gestione e Controllo: la sua adozione

Il Decreto⁵ introduce una **particolare forma di esonero della responsabilità** in oggetto qualora l'ente dimostri:

- a) di aver adottato ed efficacemente attuato attraverso l'organo dirigente, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- b) di aver affidato ad un organismo interno, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curare il loro aggiornamento;
- c) che le persone che hanno commesso il reato hanno agito eludendo fraudolentemente suddetti modelli di organizzazione e di gestione,
- d) che non vi sia omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lettera b).

1.3.1 Modello quale esimente nel caso di reato

Il Decreto prevede inoltre che, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di organizzazione, gestione e controllo debbano **rispondere alle seguenti esigenze**⁶:

- 1) individuare le aree di rischio di commissione dei reati previsti dal Decreto;
- 2) predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- 3) prevedere modalità di individuazione e di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- 4) prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- 5) configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

⁵ Art. 6, comma 1.

⁶ Art. 6, comma 2

Il Decreto dispone che i modelli di organizzazione, gestione e controllo possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (ad esempio Linee Guida) redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti può formulare (entro 30 giorni) osservazioni sulla idoneità dei modelli a prevenire i reati⁷.

E' infine previsto che, negli enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente⁸.

1.3.2 SISSI srl e l'adozione del Modello: introduzione

SISSI ritiene opportuno adeguarsi alle prescrizioni contenute nel Decreto procedendo all'adozione del Modello di Organizzazione e Gestione (di seguito Modello), al fine di prevenire la commissione di reati di cui al Decreto stesso ed assicurare, sempre più, condizioni di correttezza e trasparenza nella conduzione degli affari delle attività aziendali che lo compongono.

SISSI ha proceduto all'analisi delle aree di rischio, secondo le prescrizioni del Decreto, delle Linee Guida formulate da CONFINDUSTRIA (vedi seguente paragrafo 1.4), nonché delle recenti evoluzioni giurisprudenziali in materia.

In attuazione di quanto previsto dal Decreto, l'organo amministrativo di SISSI adotta il Modello di Organizzazione e Gestione e nomina al proprio interno un "Organismo di Vigilanza e di Controllo Interno", con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

1.4 Le Linee Guida elaborate da CONFINDUSTRIA

CONFINDUSTRIA ha approvato il testo definitivo⁹ delle proprie "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs 231/2001", che possono essere schematizzate nelle seguenti **fasi fondamentali**:

- **"identificazione dei rischi**: ossia l'analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D.Lgs 231/2001";
- **"progettazione del sistema di controllo** (c.d. **protocolli** per la programmazione della formazione ed attuazione delle decisioni dell'ente)

1.4.1 Gli aspetti essenziali delle Linee Guida di CONFINDUSTRIA

Le **componenti più rilevanti del sistema di controllo** individuate da CONFINDUSTRIA come atto a prevenire ragionevolmente la commissione dei reati previsti dal decreto sono:

- Codice Etico;
- Sistema organizzativo;
- Procedure manuali e informatiche;
- Poteri autorizzativi e di firma;
- Sistemi di controllo di gestione;
- Comunicazione al personale e sua formazione.

Le componenti del sistema di controllo devono essere uniformate ai seguenti **principi**:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (ad esempio, nessuno può gestire in autonomia un intero processo);

⁷ Art. 6, comma 3

⁸ Art. 6, comma 4

⁹ In data 7 marzo 2002 e successivamente aggiornate il 24 maggio 2004

- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
 - i. autonomia e indipendenza;
 - ii. professionalità;
 - iii. continuità d'azione;
- obblighi di informazione dell'Organismo di Vigilanza.

1.5 Evoluzione giurisprudenziale

Ai fini della redazione del Modello SISSI ha tenuto in considerazione anche i primi orientamenti giurisprudenziali che si sono formati in materia.

SISSI pertanto ha provveduto a redigere il Modello anche alla luce di queste prime decisioni giurisprudenziali, pur nella consapevolezza che le stesse non sono affatto vincolanti e che, allo stato, non hanno ancora acquisito il valore di giurisprudenza consolidata.

2 L'adozione del Modello

2.1 SISSI srl

S.I.S.S.I. S.R.L. è una società di consulenza la cui attività consiste nell'integrare nuove competenze in materia di tutela della salute e della sicurezza sul lavoro in realtà aziendali autonome, certificata Iso 9001:2008 da DNV e accreditata per la formazione Tip. SF2 dalla Regione Lombardia. E' specializzata nella consulenza per l'adeguamento o utilizzazione delle nuove norme europee e internazionali in materia di sicurezza ed igiene del lavoro, qualità, ambiente, agevolazioni per investimenti, ...) nonché nella pianificazione di interventi info-formativi studiati per adeguarsi alle necessità della popolazione interessata dai corsi e sulla base di un'attenta analisi delle esigenze dell'utente. Consapevole che il trasferimento di know-how in aziende non può avvenire senza il coinvolgimento delle persone, S.I.S.S.I. S.r.l. ha creato il proprio settore formazione il cui personale ha erogato numerosissime ore di formazione su tematiche sia tecniche che organizzative (sicurezza, tutela della salute, comunicazione, certificazione,...).

2.1.1. Mission – vedi anche la politica della qualità aggiornata annualmente nel sistema qualità

La società ha per oggetto la fornitura di servizi e la consulenza per la risoluzione delle problematiche inerenti alla salute ed alla sicurezza dei lavoratori quali, a titolo puramente esemplificativo e non tassativo: - valutazione del rischio e consulenza per la programmazione degli interventi correttivi; - piani di sicurezza, cantieri (psc), piani sostitutivi sicurezza cantieri (pss), piani operativi sicurezza cantieri (pos); - assunzione del ruolo di "responsabile del servizio di prevenzione e protezione"; - consulenza continuativa per il responsabile della sicurezza; - corsi di formazione e di informazione per lavoratori, preposti e dirigenti; - sorveglianza sanitaria con assunzione del ruolo di "medico competente"; - accertamenti sanitari di laboratorio; - sorveglianza da parte di fisico-sanitario abilitato per le radiazioni ionizzanti; - rilevazioni fonometriche e sorveglianza con strumentazione classe i; - progettazione in genere e consulenza per la realizzazione di nuovi impianti tecnologici, meccanici ed elettrici o per l'adeguamento degli impianti esistenti alle norme vigenti; - costruzione, manutenzione e gestione di manufatti e impianti in genere; - progetti e pratiche per l'ottenimento del certificato di prevenzione incendi; - progetti e pratiche i.s.p.e.s.l.; - progetti di impianti e pratiche per lo smaltimento dei rifiuti industriali in genere; - progetti di impianti e pratiche per lo scarico in atmosfera degli affluisi inquinanti; - intermediazione di carattere progettuale, tecnica e di servizi; - progetti e pratiche di valutazione di impatto ambientale; - monitoraggio ambientale di ditte e attività in genere; - indagini idrogeologiche; - pratiche relative all'i.s.o. 9000; - haccp: stesura e attuazione di procedure e strumenti di autocontrollo necessari al mantenimento del massimo livello di qualità alimentare; - pratiche sul contenimento energetico e isolamento termico strutture secondo la normativa vigente; - classificazione e valutazione di aree con pericolo di esplosione e/o incendio, secondo la normativa vigente.

*SISSI sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, nonché consapevole dell'importanza di assicurare condizioni di correttezza nella conduzione degli affari e nelle attività aziendali a tutela della posizione e dell'immagine propria e delle aspettative dei soci, **adotta il Modello di Organizzazione, Gestione e Controllo** previsto dal decreto, fissandone i principi di riferimento.*

2.1.2. Obiettivi del Modello e suoi punti cardine

Tale iniziativa, sebbene non imposta dal decreto¹⁰, si propone inoltre di sensibilizzare tutti coloro che operano in nome e/o per conto della società, affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari al fine di prevenire il rischio di commissione dei reati contemplati nel decreto stesso.

Attraverso l'individuazione delle attività esposte al rischio di reato ("**attività sensibili**") e la loro conseguente proceduralizzazione, si vuole:

- da un lato determinare una piena consapevolezza di tutti coloro che operano in nome e per conto di SISSI di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla Società, in quanto contraria ai suoi interessi anche quando, apparentemente, potrebbe trarne un vantaggio economico immediato;
- dall'altro, grazie ad un monitoraggio costante dell'attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione di reati stessi.

Punti cardine del Modello, oltre ai principi sopra riportati, sono:

- la mappatura delle attività a rischio, ossia quelle attività nel cui ambito è più probabile la commissione dei reati previsti dal Decreto, le "attività sensibili" appunto;
- l'attribuzione all'Organismo di Vigilanza di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- la verifica e la documentazione di ogni operazione rilevante;
- l'attribuzione di poteri coerenti con le responsabilità organizzative;
- la diffusione ed il coinvolgimento di tutti i livelli aziendali nell'attuazione di regole comportamentali, procedure e politiche aziendali.

2.1.3 Struttura del Modello: Parte Generale e Parte Speciale

Il Modello è suddiviso nelle seguenti parti:

- **Parte Generale**, che contiene i punti cardine del Modello e tratta del funzionamento dell'Organismo di Vigilanza e del sistema sanzionatorio, facendo peraltro rinvio al Codice Etico;
- **Parte Speciale**, il cui contenuto è costituito dalle diverse tipologie di reato previste dal Decreto, ossia i reati realizzabili nei rapporti con la Pubblica Amministrazione, i reati societari, i reati informatici e trattamento illecito di dati, i reati di omicidio colposo e lesioni colpose gravi e gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, i reati contro la tutela dei diritti d'autore. Infine l'ultimo capitolo è dedicato alle "Attività strumentali alla commissione dei reati".

Nell'eventualità in cui si rendesse necessario procedere all'integrazione della Parte Speciale, relativamente a nuove fattispecie di reato che fossero in futuro incluse nell'ambito di applicazione del Decreto, è demandato all'organo amministrativo della società il potere di integrare il presente Modello in una fase successiva, mediante apposita delibera.

2.1.4 Approvazione del Modello

Il presente Modello, il Regolamento e lo Statuto dell'OdV, il Codice Etico e il Sistema Disciplinare, è stato approvato dall'Amministratore Unico di SISSI **in data 10 Marzo 2011**.

¹⁰ Che indicano il Modello come elemento facoltativo e non obbligatorio

2.1.5 Modifiche e aggiornamento del Modello

Come sancito dal Decreto, il Modello è "atto di emanazione dell'organo dirigente"¹¹. Di conseguenza le successive modifiche nonché eventuali integrazioni sostanziali sono rimesse alle competenze dell'Amministratore Unico di SISSI.

Tuttavia è riconosciuta, in via generale, all' **Amministratore SISSI** – previa informativa all'Organismo di Vigilanza – la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale.

2.2 Approccio metodologico al Modello

Ai fini della redazione ed implementazione del Modello organizzativo e di gestione ex D.Lgs n. 231/2001, l'approccio metodologico adottato ha previsto le seguenti fasi:

- individuazione delle aree potenzialmente esposte al rischio di commissione di reati;
- "risk assessment" dei processi inerenti alle aree di rischio individuate, con descrizione delle relative criticità eventualmente riscontrate;
- individuazione di soluzioni ed azioni volte al superamento o alla mitigazione delle criticità rilevate;
- adeguamento e stesura di procedure organizzative sulle aree individuate e potenzialmente a rischio, contenenti disposizioni vincolanti ai fini della ragionevole prevenzione delle irregolarità di cui al Decreto;
- elaborazione del Codice Etico;
- redazione di un sistema disciplinare per sanzionare il mancato rispetto delle misure indicate nel Modello;
- regolamento dell'Organismo di Vigilanza;
- piano di formazione e comunicazione del Modello.

2.2.1 La metodologia di risk assessment

L'efficace esecuzione del progetto e l'esigenza di adottare criteri oggettivi, trasparenti e tracciabili per la costruzione del Modello organizzativo ha richiesto l'utilizzo di adeguate metodologie e di strumenti tra loro integrati. Gli elementi sopra evidenziati sono sinteticamente descritti a seguire, insieme ad una sintesi delle valutazioni che sono state svolte:

Governo

In quest'ambito sono state esaminate le modalità di attribuzione delle competenze degli organi interessati alla gestione dei sistemi di controllo interno.

Codice etico e procedure operative

In questo ambito sono stati esaminati i sistemi organizzativi adottati al fine di verificarne la coerenza con le risultanze del processo di "risk assessment", con norme e regolamenti, con l'attuale assetto organizzativo, con la metodologia di gestione dei processi aziendali e delle risorse umane.

Comunicazione

In tale ambito è stato esaminato il sistema di comunicazione interna in relazione agli elementi del Modello e, in particolare, all'adeguatezza dei contenuti, dei canali utilizzati, della periodicità/frequenza della comunicazione, della differenziazione per gerarchia, funzione e livelli di rischio ed alla comprensibilità del linguaggio.

Formazione

In tale ambito sono state esaminate le procedure e le prassi utilizzate per la formazione del personale sull'applicazione del Modello, sia nel quadro dei programmi a contenuto generale specifici sviluppati o da sviluppare, per gli addetti alle aree di rischio.

¹¹ Art. 6, comma 1, lettera a) del Decreto.

Risorse umane

In tale ambito sono state esaminate le prassi e le procedure utilizzate per la gestione delle risorse umane nel regolare i principali aspetti del rapporto di lavoro dipendente; saranno valutati anche gli altri aspetti qualificanti in chiave di prevenzione degli illeciti, quali, ad esempio, i sistemi di incentivazione e quelli dissuasivi e sanzionatori, tra cui l'allontanamento del personale, specificati dalla Legge.

Controllo

In tale ambito sono state esaminate le prassi e le procedure utilizzate per le attività di controllo e di monitoraggio delle performance degli elementi del Modello; quindi sarà esaminata l'adeguatezza del processi di controllo delle aree e delle operazioni a rischio attraverso segnali premonitori, anomalie, controlli di routine nelle aree a rischio ed infine della adeguatezza del Modello.

Informazione

In questo ambito sono state esaminate le caratteristiche e le modalità di generazione, accesso e reporting direzionale delle informazioni necessarie per un'efficace vigilanza sui rischi da parte degli organismi interessati e, in primo luogo, da parte dell'Organismo di Vigilanza previsto dal Decreto; pertanto è stata esaminata la disponibilità dei dati necessari per l'esercizio di un'efficace vigilanza preventiva e successiva sulle attività a rischio, l'esistenza di canali di comunicazione preferenziali per la segnalazione di operazioni esposte a rischio, sia da parte di terzi che da parte del personale, la tempestiva segnalazione del cambiamento dei profili del rischio; nonché la regolare registrazione e reporting degli eventi sopradescritti, con le relative azioni successive implementate e l'esito dei controlli svolti.

Violazioni

In questo ambito sono state analizzate le caratteristiche e le modalità di effettuazione delle attività di audit e/o di investigazione interna ed esterna, al fine di verificarne l'efficacia sia in termini di standard professionali e/o qualitativi, sia in termini di effetto sull'aggiornamento degli elementi del sistema di controllo interno e di "corporate governance".

2.2.2 Fasi operative

L'approccio metodologico adottato è stato implementato e sviluppato attraverso una serie di fasi operative. L'inizio di tale attività ha richiesto una preventiva acquisizione di dati ed informazioni sul sistema organizzativo della Società e sui processi operativi, utili ai fini della pianificazione di dettaglio delle singole fasi. L'implementazione della suddetta metodologia si è articolata nelle seguenti fasi:

- Pianificazione, Diagnosi, Progettazione, Predisposizione, Implementazione.

Fase 1: Pianificazione

In questa fase abbiamo proceduto alla raccolta della documentazione ed al reperimento delle informazioni utili alla conoscenza dell'attività e del sistema organizzativo della Società.

Tali informazioni riguardano, tra l'altro, a mero titolo informativo:

- i settori economici in cui la Società opera;
- la tipologia delle relazioni e delle attività intrattenute con le Pubbliche Amministrazioni, italiane o estere;
- i casi di eventuali presunte irregolarità avvenute in passato;
- il quadro regolamentare e procedurale interno (ad esempio: deleghe di funzioni, processi decisionali, procedure operative ISO o non ISO, protocolli);
- la documentazione inerente ordini di servizio, comunicazioni interne ed ogni altra evidenza documentale utile alla migliore comprensione delle attività svolte dalla Società e del sistema organizzativo.

Fase 2: Diagnosi

In sintesi l'analisi delle predette componenti si è incentrata:

- sulla verifica dell'adeguatezza del sistema organizzativo, seguendo i criteri di:
 - formalizzazione del sistema;
 - chiara definizione delle responsabilità attribuite e delle linee di dipendenza gerarchica;
 - esistenza della contrapposizione di funzioni;
 - corrispondenza tra le attività effettivamente svolte e quanto previsto dalle missioni e responsabilità descritte nell'organigramma della società e nel MAQ
- sulla verifica dell'esistenza dei protocolli e delle procedure formalizzate per regolamentare le attività svolte dalle strutture nelle aree potenzialmente a rischio, tenendo conto delle fasi di istruzione e formazione delle decisioni aziendali;
- sulla verifica dell'esistenza di poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate e/o concretamente svolte. (L'accertamento è stato condotto sulla base dell'esame delle procure rilasciate e delle deleghe gestionali interne /sistema autorizzativi alla spesa ed a contrattare);
- sulla verifica, per le singole attività potenzialmente a rischio reato, dell'esistenza di protocolli, procedure e di regole di comportamento, individuando le integrazioni necessarie per una maggior aderenza ai principi espressi dal D.Lgs. n. 231/2001;
- sulla verifica dell'adeguatezza del sistema disciplinare vigente diretto a sanzionare l'eventuale violazione dei principi e delle disposizioni volte a prevenire la commissione dei reati, sia da parte dei dipendenti della società – dirigenti e non – sia da parte di Amministratori e collaboratori esterni;
- sulla verifica dell'esistenza di forme di comunicazione e formazione per il personale, in considerazione della necessità che, iniziative dirette a dare attuazione al D.Lgs n. 231/2001, debbano essere programmate e finalizzate alla comunicazione del Modello organizzativo.

I risultati ottenuti dalla suddetta analisi hanno costituito la base per la progettazione del Modello organizzativo, così come di seguito specificato.

Fase 3: Progettazione

Tale fase ha riguardato:

- la verifica/censimento di protocolli, procedure operative e/o strumenti di controllo già esistenti per ciascuna area potenzialmente a rischio. In particolare:
 - i. sono stati rilevati gli aspetti di criticità e di carenza nei sistemi di controllo esistenti nell'ottica di prevenire ragionevolmente le ipotesi di reato previste dal Decreto;
 - ii. sono state formulate raccomandazioni, suggerimenti e linee guida sulle integrazioni e miglioramenti da apportare in modo da superare ragionevolmente le criticità rilevate.

La progettazione del sistema di *reporting* informativo consente all'Organismo di Vigilanza di ricevere informazioni ed aggiornamenti sullo stato delle attività risultate potenzialmente esposte a rischio.

Fase 4: Predisposizione

Tale fase ha condotto alla redazione del Modello organizzativo mediante la materiale predisposizione e/o adattamento degli strumenti organizzativi di cui si compone, ritenuti più opportuni a valorizzare l'efficacia dell'azione di prevenzione dei reati, come nella:

- redazione e revisione delle procedure operative per le aree/attività ritenute potenzialmente a rischio in quanto prive di presidi di controllo;
- elaborazione del codice etico e quindi di principi etici per le aree/attività ritenute potenzialmente a rischio in quanto prive di presidi di controllo;
- definizione dei poteri, compiti e responsabilità dell'Organismo di vigilanza e suoi rapporti con le strutture aziendali;

- progettazione delle iniziative in tema di comunicazione e di formazione etica e prevenzione dei reati.

Fase 5: Implementazione

In tale fase l'attività condotta ha l'obiettivo di rendere operativo il Modello nel suo complesso, mediante:

- la sua formale adozione a mezzo approvazione da parte dell'Amministratore Unico;
- la definitiva attuazione e comunicazione degli elementi di cui esso si compone: codice etico, procedure operative, organismo di vigilanza, piano di comunicazione e formazione, sistema disciplinare.

2.3 Il Modello ed il Codice Etico a confronto

Il Modello risponde all'esigenza di prevenire, per quanto possibile, la commissione di reati previsti dal Decreto attraverso la predisposizione di regole di comportamento specifiche.

I comportamenti di dipendenti e amministratori ("Dipendenti"), di coloro che agiscono, anche nel ruolo di consulenti o comunque con poteri di rappresentanza della società ("Consulenti") e delle altre controparti contrattuali di SISSI, quali ad esempio eventuali partner in joint venture, ATI etc ("partner"), devono conformarsi alle regole di condotta – sia generali sia specifiche – previste nel Modello e nel Codice Etico.

SISSI Srl, rilevato che la gran parte dell'attività aziendale viene svolto da consulenti esterni, ha deciso di coinvolgere anche questi ultimi nelle previsioni del presente modello cercando di perseguire la gestione maggiormente efficiente nella previsione e prevenzione dei reati previsti dal D.Lgs 231/01.

In particolare:

- I Dipendenti, i Consulenti e i Partner non devono porre in essere quei comportamenti:
 - che integrano le fattispecie di reato previste dal Decreto;
 - che, sebbene non costituiscano di per sé un'ipotesi di reato, possano agevolare la commissione o possano potenzialmente costituire una vera e propria ipotesi di reato;
- I Dipendenti, i Consulenti e i Partner devono evitare di porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione;
- È fatto divieto di effettuare elargizioni in denaro a pubblici funzionari;
- È obbligatorio il rispetto della prassi aziendale per la distribuzione di omaggi e regali;
- I rapporti nei confronti della Pubblica Amministrazione devono essere gestiti in modo unitario, intendendosi con ciò che le persone che rappresentano la Società nei confronti della Pubblica Amministrazione devono aver ricevuto un esplicito mandato da parte dell'Azienda;
- Coloro che svolgono una funzione di controllo e supervisione verso i Dipendenti che operano con enti pubblici devono seguire con attenzione e con le modalità più opportune l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- I compensi dei Consulenti e dei Partner devono essere determinati solo per iscritto;
- Nessun tipo di pagamento può essere effettuato in contanti o in natura se superiore a 5.000 euro;
- Devono essere istituite, da parte degli Amministratori, e immediatamente comunicate all'Organismo di Vigilanza apposite procedure per consentire l'esercizio del controllo nei limiti previsti (ai soci, agli altri organi, alle società di revisione) e il rapido accesso alle informazioni attribuite da leggi e regolamenti.

2.4 I destinatari del Modello

Le regole contenute nel Modello si applicano a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo della Società, ai dipendenti, nonché a coloro i quali, pur non appartenendo all'azienda, operano su mandato della medesima o sono legati alla Società da rapporti aventi carattere di continuità.

SISSI comunica il presente Modello attraverso modalità idonee ad assicurarne l'effettiva conoscenza da parte di tutti i dipendenti. I soggetti ai quali il Modello si rivolge sono tenuti a rispettarne puntualmente tutte le

disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società.

SISSI condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello e del Codice Etico, anche qualora il comportamento sia realizzato nell'interesse della Società ovvero con l'intenzione di arrecare ad essa un vantaggio.

3 L'Organismo di Vigilanza

Nel caso in cui si verificano fatti integranti i reati previsti il Decreto¹² pone come condizione per la concessione dell'esimente dalla responsabilità amministrativa che sia stato affidato a un organismo dell'Ente (dotato di autonomi poteri di iniziativa e di controllo) il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

3.1 Identificazione dell'Organismo di Vigilanza interno

In attuazione di quanto previsto dal decreto, l'organismo cui affidare tale compito è stato individuato nelle figure di MARIA MAGDA POLENGHI – ALESSANDRO CORDONI in qualità di membri interni e di due membri esterni in qualità di autorità di supervisione nelle persone dell'Avv. Paolo Lessio del Foro di Milano e del Dott. Maurizio Prati nonché dell'Amministratore Unico DANIELE CORDONI.

3.2 Funzioni e poteri

All'Organismo di Vigilanza è affidato il **compito di vigilare** sull':

- **Effettività** del Modello: ossia vigilare affinché i comportamenti posti in essere all'interno dell'Azienda corrispondano al modello predisposto;
- **Efficacia** del Modello: ossia verificare che il Modello predisposto sia concretamente idoneo a prevenire il verificarsi dei reati previsti dal Decreto e dai successivi provvedimenti che modificano il campo di applicazione;
- **Opportunità di aggiornamento** del Modello al fine di adeguarlo ai mutamenti ambientali e alle modifiche della struttura aziendale.

Su di un piano più operativo è affidato all'Organismo di Vigilanza il compito di:

- Verificare periodicamente la mappa delle aree di rischio reato (o attività sensibili) al fine di adeguarla ai mutamenti dell'attività e/o della struttura aziendale. A tal fine all'Organismo di Vigilanza devono essere segnalate da parte del management e da parte degli addetti alle attività di controllo nell'ambito delle singole funzioni, le eventuali situazioni che possono esporre l'Azienda a rischi di reato. Tutte le comunicazioni devono essere esclusivamente in forma scritta;
- Verificare l'adeguatezza e l'efficacia del Modello nella prevenzione dei reati di cui al Decreto;
- Effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere, soprattutto, nell'ambito delle attività sensibili i cui risultati vengano riassunti in un apposito rapporto il cui contenuto sarà esposto nel corso delle comunicazioni agli organi societari;
- Coordinarsi con i consulenti esterni attraverso apposite riunioni e scambi e-mail per la trasmissione delle informazioni per tenere aggiornate le aree a rischio reato per:
 - Tenere sotto controllo la loro evoluzione al fine di realizzare il costante monitoraggio;
 - Verificare i diversi aspetti attinenti l'attuazione del Modello (definizione di clausole standard, formazione del personale, cambiamenti normativi ed organizzativi, etc);
 - Garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace siano intraprese tempestivamente;
- Raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute nel rispetto del Modello, nonché aggiornare la lista delle informazioni che allo stesso devono essere trasmesse. A tal fine l'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale rilevante e deve essere costantemente informato dal management;

¹² Art. 6, lett. b).

- Promuovere iniziative per la formazione e la comunicazione del Modello e predisporre la documentazione necessaria a tal fine;
- Interpretare la normativa rilevante e verificare l'adeguatezza del sistema di controllo interno in relazione a tali prescrizioni normative;

La struttura così identificata deve essere in grado di agire nel rispetto dell'esigenza di recepimento, verifica e attuazione dei Modelli richiesti dall'art. 6 del decreto, ma anche, necessariamente, rispetto all'esigenza di costante monitoraggio dello stato di attuazione e della effettiva rispondenza degli stessi modelli alle esigenze di prevenzione che la legge richiede. Tale attività di costante verifica deve tendere in una duplice direzione:

- Qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente, è compito dell'Organismo di Vigilanza adottare tutte le iniziative necessarie per correggere questa situazione. Si tratterà allora, a seconda dei casi e delle circostanze, di:
 - Sollecitare i responsabili delle singole unità organizzative al rispetto del Modello di comportamento;
 - Indicare direttamente quali correzioni e modificazioni debbano essere apportate alle ordinarie prassi di attività;
 - Segnalare i casi più gravi di mancata attuazione del Modello ai responsabili e agli addetti ai controlli all'interno delle singole funzioni;
- Qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di adeguamento, che pertanto risulti integralmente e correttamente attuato, ma si riveli non idoneo allo scopo di evitare il rischio di verificarsi di taluno dei reati previsti dal decreto, sarà proprio l'Organismo di Vigilanza a doversi attivare per garantire l'aggiornamento nonché i tempi e le forme dell'adeguamento.¹³

A tal fine, come anticipato, l'Organismo di Vigilanza deve avere libero accesso alle persone e a tutta la documentazione aziendale e la possibilità di acquisire dati e informazioni rilevanti dai soggetti responsabili. Infine all'Organismo di Vigilanza devono essere segnalate tutte le informazioni come di seguito specificato.

3.3 Reporting dell'Organismo di Vigilanza agli Organi Societari

L'Organismo di Vigilanza ha la responsabilità nei confronti dell'organo amministrativo di comunicare:

- Periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli;
- Immediatamente eventuali problematiche significative scaturite dalle attività;
- Almeno annualmente in merito all'attuazione del modello da parte della Società.

L'Organismo di Vigilanza potrà essere invitato a relazione periodicamente all'Amministratore Unico in merito alle proprie attività.

L'Organismo di Vigilanza deve inoltre, valutando le singole circostanze:

1. Comunicare i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'Organismo di Vigilanza ottenga dai responsabili dei processi un piano delle azioni, con relativa tempistica, per le attività suscettibili di miglioramento, nonché le specifiche delle modifiche necessarie per realizzare l'implementazione;
2. Segnalare eventuali comportamenti/azioni non in linea con il Codice Etico e con le procedure e/o protocolli aziendali, al fine di:
 - a. Acquisire tutti gli elementi per effettuare comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
 - b. Evitare il ripetersi dell'accadimento, dando indicazioni per la rimozione delle carenze.

Le attività indicate al punto 2) dovranno essere comunicate dall'Organismo di Vigilanza all'Amministratore Unico nel più breve tempo possibile, richiedendo anche il supporto di altre strutture aziendali, che possano

¹³ Tempi e forme, naturalmente, non predeterminati. I tempi devono comunque intendersi come i più solleciti possibile e il contenuto sarà quello imposto dalle rilevazioni che hanno determinato l'esigenza di adeguamento.

collaborare nell'attività di accertamento e nell'individuazione delle azioni volte a impedire il ripetersi di tali circostanze.

Le copie dei relativi verbali saranno custodite dall'Organismo di Vigilanza e dagli organismi di volta in volta coinvolti.

3.4 Reporting: prescrizioni generali e prescrizioni specifiche obbligatorie

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei soggetti tenuti all'osservanza del Modello, in merito a eventi che potrebbero ingenerare responsabilità di SISSI ai sensi del Decreto.

3.4.1 Prescrizioni di carattere generale

Valgono al riguardo le seguenti prescrizioni di carattere generale:

- Devono essere raccolte da ciascun Responsabile di Funzione eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati contemplati dal Decreto o comunque a comportamenti in generale non in linea con le regole di comportamento di cui al Modello;
- Ciascun dipendente deve segnalare la violazione (o presunta violazione) del Modello contattando il proprio diretto superiore gerarchico e/o l'Organismo di Vigilanza (con disposizione dell'Organismo di Vigilanza sono istituiti eventualmente "canali informativi dedicati" per facilitare il flusso di segnalazioni / informazioni ufficiose);
- I consulenti, i collaboratori ed i partner, per quanto concerne la loro attività svolta nei confronti di SISSI, effettuano le segnalazioni direttamente all'Organismo di Vigilanza mediante "canali informativi dedicati" che sarà compito dell'Organismo di Vigilanza stessa definire;
- L'Organismo di Vigilanza valuta le segnalazioni ricevute e le attività da porre in essere; gli eventuali provvedimenti conseguenti sono definiti e applicati in conformità a quanto infra previsto in ordine al sistema disciplinare.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione e, in ogni caso, sarà assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti di SISSI o delle persone accusate in mala fede.

3.4.2 Prescrizioni specifiche obbligatorie

Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere trasmesse all'Organismo di Vigilanza le notizie relative:

- Ai procedimenti penali e disciplinari azionati in relazione a notizia di violazione del Modello;
- Alle sanzioni irrogate (ivi compresi i provvedimenti assunti verso i dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- Alle ispezioni o iniziative di qualsivoglia autorità pubblica di vigilanza.

3.4.3 Reporting da parte di esponenti aziendali o di terzi

In ambito aziendale dovrà essere portata a conoscenza dell'Organismo di Vigilanza, oltre alla documentazione prescritta nella Parte Speciale del Modello secondo le procedure ivi contemplate, ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi e attinente all'attuazione del Modello nelle aree di attività a rischio.

3.5 Raccolta, conservazione e archiviazione delle informazioni

Ogni informazione, segnalazione, report previsti dal Modello sono conservati dall'Organismo di Vigilanza in un apposito database informativo e/o cartaceo. (SISSI 231). Le informazioni sono a disposizione di soggetti esterni all'Organismo di Vigilanza previa autorizzazione dell'Organismo stesso. Quest'ultimo definisce con apposita disposizione interna criteri e condizioni di accesso al database

3.6 Statuto dell'Organismo di Vigilanza

Vedi Statuto dell'organismo di Vigilanza SISSI

3.7 Regolamento dell'Organismo di Vigilanza

Vedi Regolamento dell'organismo di Vigilanza SISSI

4 Formazione e diffusione del Modello

4.1 Dipendenti

4.1.1 Formazione dei dipendenti

SISSI riconosce e ritiene che, ai fini dell'efficacia del presente Modello, sia necessario garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute sia nei confronti dei Dipendenti di sede che dei c.d. "esterni". La formazione è gestita dall'Organismo di Vigilanza in stretta collaborazione con il vertice aziendale, con il responsabile del personale e con il RAQ. La formazione potrà essere articolata con seminari; occasionali e-mail di aggiornamento; informativa con la lettera di assunzione per i neo-assunti; con nota informativa interna o, in ogni caso, mediante modalità che saranno ritenute idonee in base al livello ed al ruolo ricoperto dal singolo Dipendente, nonché in relazione al differente coinvolgimento dello stesso nelle "attività sensibili".

4.2 Collaboratori Esterni e partner

4.2.1 Informativa a Collaboratori Esterni e Partner

In linea con la politica di SISSI di coinvolgimento dei collaboratori esterni verranno fornite a questi ultimi apposite informative sulle politiche e le procedure adottate sulla base del presente Modello organizzativo, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

5 Il sistema disciplinare

5.1 Principi generali

Ai sensi degli artt. 6, comma 2, lett. e) e 7, comma 4, lett. b) del Decreto il Modello può ritenersi efficacemente attuato solo qualora preveda un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in esso indicate.

Tale sistema disciplinare si rivolge ai dipendenti ed ai dirigenti, prevedendo adeguate sanzioni di carattere disciplinare. La violazione delle regole di comportamento del Codice Etico e delle misure previste dal Modello, da parte di lavoratori dipendenti dell'Azienda e/o dei dirigenti della stessa, costituisce un inadempimento alle obbligazioni del rapporto di lavoro, ai sensi dell'art. 2104 c.c. e dell'art. 2106 c.c. .

Le infrazioni dei principi sanciti nel Codice Etico e delle misure previste dal Modello, le relative sanzioni irrogabili e il procedimento disciplinare sono descritti nella sezione specifica del Codice Etico, approvato dall'Amministratore DANIELE CORDONI e successivamente dall'Assemblea dei Soci. L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta, i protocolli e le procedure interne sono vincolanti per i destinatari, indipendentemente dall'effettiva realizzazione di un reato quale conseguenza del comportamento commesso.

5.2 Misure nei confronti dei Dipendenti

L'art. 2104 c.c. , individuando il dovere di "obbedienza" a carico del lavoratore, dispone che il prestatore di lavoro deve osservare nello svolgimento del proprio lavoro le disposizioni di natura sia legale che contrattuale impartite dal datore di lavoro. In caso di inosservanza di dette disposizioni il datore di lavoro può irrogare sanzioni disciplinari, graduate secondo la gravità dell'infrazione, nel rispetto delle previsioni contenute nel CCNL applicabile. In particolare il sistema disciplinare deve risultare conforme ai seguenti **principi**:

- Il sistema deve essere debitamente pubblicizzato mediante affissione in luogo accessibile ai dipendenti ed eventualmente oggetto di specifici corsi di aggiornamento e di informazione;

5.3 Misure nei confronti degli Amministratori

In caso di violazione della normativa vigente, del Modello o del Codice Etico da parte degli Amministratori di SISSI, l'Organismo di Vigilanza informa l'Assemblea dei soci, la quale provvede ad assumere le opportune iniziative previste dalla vigente normativa.

5.4 Misure nei confronti di soggetti esterni

Ogni comportamento posto in essere da collaboratori, consulenti o altri terzi collegati a SISSI da un rapporto contrattuale non di lavoro dipendente, in violazione delle previsioni del Modello e/o del Codice Etico, potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o anche in loro assenza, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla società, anche indipendentemente dalla risoluzione del rapporto contrattuale.

5.5 Sistema Disciplinare

Si adotta quello previsto dal decreto.

Parte Speciale

Introduzione

Nella Parte Speciale, che segue, saranno analizzate le attività considerate come "sensibili" ai fini del Decreto in relazione al tipo di attività di SSSI. Saranno in particolare analizzate le attività che presentano profili di rischio in relazione alle seguenti tipologie di reato:

1. Reati contro la Pubblica Amministrazione;
2. Reati societari;
3. Delitti informatici e trattamento illecito di dati;
4. Reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
5. Reati contro la tutela dei diritti d'autore;
6. Attività strumentali alla commissione dei reati.

6 Reati contro la Pubblica Amministrazione

6.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione

Per quanto riguarda la presente Parte Speciale si provvede qui di seguito a fornire una breve descrizione dei reati contemplati dagli artt. 24 e 25 del decreto, facendo un rimando al paragrafo 1.1.4 della Parte generale per definizione ed esempi relativi ai concetti di Pubblica Amministrazione, funzione pubblica, pubblico ufficiale, pubblico servizio e persona incaricata di pubblico servizio.

Malversazione a danno dello Stato, di altro ente pubblico o delle Comunità Europee (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo aver ricevuto finanziamenti o contributi da parte dello Stato o di altro ente pubblico o delle Comunità Europee, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non siano destinati alle finalità per cui erano stati erogati.

Indebita percezione di erogazioni in danno dello Stato, di altro ente pubblico o delle Comunità Europee (art. 316-ter c.p.)

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

In questo caso, a differenza di quanto visto al punto precedente, a nulla rileva l'uso fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Inoltre va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa in danno dei medesimi soggetti, nel senso che la punibilità a questo titolo è configurabile solo nei casi in cui non lo sia a titolo della predetta ipotesi di truffa.

Concussione (art. 317 c.p.)

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

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318 e 319 c.p.)

Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio riceva, per sé o per altri, denaro o altri vantaggi per compiere atti contrari al proprio ufficio, ovvero per compiere, omettere o ritardare atti del proprio ufficio (determinando un vantaggio a favore del corruttore).

Si ricorda che il reato di corruzione è un reato a concorso necessario, in cui sono puniti sia il corrotto che il corruttore (cfr. art. 321 c.p.).

La corruzione c.d. propria, quella per il compimento di un atto contrario ai doveri di ufficio (ad esempio, accettazione di denaro per garantire l'aggiudicazione di una gara) può essere commessa da un pubblico ufficiale e da un incaricato di pubblico servizio; mentre la corruzione c.d. impropria, quella per il compimento di un atto dovuto (ad esempio velocizzare una pratica la cui evasione è di propria competenza) può essere commessa da un pubblico ufficiale e da un incaricato di pubblico servizio che rivesta la qualità di pubblico impiegato. Possono configurarsi sia corruzioni c.d. attive (l'amministratore o il dipendente corrompono un pubblico ufficiale o un incaricato di pubblico servizio per ottenere un vantaggio per la società) sia corruzioni c.d. passive (l'esponente della società riceve denaro o altra utilità per compiere un atto dovuto o contrario ai doveri d'ufficio), nei casi in cui l'attività svolta in concreto debba essere qualificata come pubblica funzione o pubblico servizio.

Tale ipotesi di reato si differenzia dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato è mero soggetto passivo, che subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o l'incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatogli (anche in tal caso, ove si tratti di istigazione alla corruzione impropria, l'incaricato di pubblico servizio deve rivestire, nel contempo, anche la qualifica di pubblico impiegato, non necessario nel caso di istigazione alla corruzione propria).

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

Tale ipotesi di reato può venire in rilievo in quei casi in cui l'ente sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, tramite un proprio esponente, corrompa un pubblico ufficiale (non solo un magistrato ma anche un cancelliere o un altro funzionario)

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

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 un danno allo Stato (oppure ad altro ente pubblico o all'Unione Europea).

Tale reato può realizzarsi, ad esempio, qualora nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere supportate da documentazione artefatta al fine di ottenere l'aggiudicazione della gara stessa.

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

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

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

Frode informatica (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informativo o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o a un altro ente pubblico.

Il reato può essere integrato, ad esempio, qualora una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

6.2 Aree di attività a rischio ("attività sensibili")

I reati sopra considerati hanno come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato) e lo svolgimento di attività concretanti una pubblica funzione o un pubblico servizio. Per definizioni, maggiori approfondimenti ed esempi specifici si rimanda alla Parte Generale del Modello.

Le seguenti aree sono state ritenute più specificatamente a rischio a conclusione dell'attività di autovalutazione condotta internamente.

ATTIVITA'	RESPONSABILITA' INTERNA SISSI	SISTEMI DI CONTROLLO UTILIZZATI
Partecipazione a procedure ad evidenza pubblica (gare, appalti)	Amministratore Unico	Codice etico L'amministratore decide la partecipazione alla gara o alla richiesta di accesso al contributo e sottopone l'ipotesi di lavoro al CdA e all'OdV affinché quest'ultimo possa modificare adeguatamente il modello organizzativo
Gestione dei rapporti di natura istituzionale con gli Enti Locali	Responsabile Amministrativo	Codice Etico Obbligo di uso della PEC nelle comunicazioni con la PA a fini di trasparenza e rintracciabilità
Gestione dei rapporti con Agenzia delle Entrate e Guardia di Finanza in occasione di visite ispettive in materia tributaria e fiscale	Responsabile Amministrativo	Codice Etico PG RAPPORTI CON LA PA IN MATERIA DI LAVORO, PREVIDENZA, SICUREZZA E FISCALE (all. 1)
Gestione dei rapporti con INPS e INAIL in occasione di visite ispettive in materia di lavoro e adempimenti previsti dalla legge	Responsabile Amministrativo	Codice Etico PG RAPPORTI CON LA PA IN MATERIA DI LAVORO, PREVIDENZA, SICUREZZA E FISCALE (all. 1)
Gestione dei rapporti con la Direzione Provinciale del Lavoro e Tribunale per i contenziosi con i lavoratori	Responsabile Amministrativo	Codice Etico PG RAPPORTI CON LA PA IN MATERIA DI LAVORO, PREVIDENZA, SICUREZZA E FISCALE (all. 1)
Gestione dei rapporti con l'Autorità Giudiziaria per i contenziosi	Legale Rappresentante	Codice Etico
Gestione dei rapporti con l'Agenzia delle Entrate per invio documentazione e richiesta informazioni	Responsabile Amministrativo	Codice Etico PG RAPPORTI CON LA PA IN MATERIA DI LAVORO, PREVIDENZA, SICUREZZA E FISCALE (all. 1)
Adempimenti inerenti la privacy	Legale Rappresentante	Codice Etico
Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali	Responsabile Amministrativo	Codice Etico Obbligo di uso della PEC nelle comunicazioni con la PA a fini di trasparenza e rintracciabilità
Gestione di liquidità	Responsabile Amministrativo	Codice Etico
Gestione di pagamenti e acquisti di beni e servizi	Responsabile Amministrativo	Codice Etico All. 2 e 5

Eventuali integrazioni delle suddette aree di attività a rischio o "attività sensibili" potranno essere disposte dall' Amministratore Unico di SISSI previo concerto con l'Organismo di Vigilanza, al quale è dato mandato di definire gli opportuni provvedimenti operativi.

6.3 Destinatari della Parte Speciale

Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

6.4 Principi generali di comportamento

La presente Parte Speciale prevede l'**espresso obbligo**, a carico degli Esponenti Aziendali in via diretta e, tramite apposite clausole contrattuali, a carico dei Collaboratori esterni e dei Partner, di:

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

La presente Parte Speciale prevede, conseguentemente, l'**espresso divieto** a carico degli Esponenti Aziendali in via diretta e a carico dei Collaboratori Esterni e Partner, di:

1. agire comportamenti tali da integrare le fattispecie di reato sopra considerate (Artt. 24 e 25 del Decreto);
2. agire comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra elencate possano potenzialmente diventarlo;

Nell'ambito dei suddetti comportamenti, in particolare, anche per il tramite di società controllate, collegate e/o collaboratori:

1. è vietato tenere rapporti con la Pubblica Amministrazione se non da parte dei soggetti a ciò deputati secondo l'organigramma della società (indicante da MAQ anche le funzioni svolte), ordini di servizio o eventuali deleghe;
2. è fatto divieto di offrire o effettuare, direttamente o indirettamente, pagamenti indebiti e promesse di vantaggi personali, di qualsiasi natura, ai rappresentanti della Pubblica Amministrazione italiana e straniera. Tale divieto include l'offerta, diretta o indiretta, di gratuita disponibilità di servizi, finalizzata a influenzare decisioni o transazioni;
3. è vietato distribuire ai rappresentanti della Pubblica Amministrazione omaggi o regali, salvo che si tratti di piccoli omaggi di modico (inferiore a 50 Euro) o simbolico valore e, in ogni caso, tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere considerati finalizzati all'acquisizione impropria di benefici;
4. è vietato presentare ad organismi pubblici nazionali o stranieri dichiarazioni non veritiere o prive delle informazioni dovute nell'ottenimento di finanziamenti pubblici e, in ogni caso, compiere qualsivoglia atto che possa trarre in inganno l'ente pubblico nella concessione di erogazioni o effettuazioni di pagamenti di qualsiasi natura;
5. è vietato ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico funzionario, tali da influenzare le conclusioni dell'attività amministrativa;
6. è vietato riconoscere compensi a consulenti, collaboratori o partner commerciali della Società che non trovino giustificazione nelle attività effettivamente prestate;
7. è vietato alterare in qualsiasi modo i sistemi informatici e telematici della Società o manipolarne i dati.

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

1. effettuare elargizioni in denaro a pubblici funzionari;
2. distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali e di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda.

Come previsto dal Codice Etico, gli omaggi consentiti si caratterizzano sempre per esiguità del valore o perché volti a promuovere l'immagine ed il marchio della società. Tutti i regali offerti – salvo quelli di modico valore – devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo;

3. accordare altri vantaggi di qualsiasi natura (promesse di assunzione etc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto 2);
4. effettuare prestazioni in favore dei partner che non trovino adeguata giustificazione nel contesto del rapporto associativo costituito con i partner stessi;
5. riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
6. ricevere o sollecitare elargizioni in denaro, omaggi o vantaggi di altra natura, nell'ambito dell'esercizio di pubbliche funzioni o di pubblico servizio; chiunque riceve omaggi o vantaggi di altra natura non compresi nelle fattispecie consentite è tenuto, secondo le procedure stabilite, a darne comunicazione all'Organismo di Vigilanza, che ne valuta l'appropriatezza e provvede a far notificare a chi ha elargito tali omaggi la politica di SISSI in materia;
7. presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
8. destinare somme ricevute da organismi pubblici e nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopo diversi da quelli cui erano destinati;
9. conferire incarichi di consulenza a soggetti segnalati dalla Pubblica Amministrazione.

6.5 Principi di attuazione dei comportamenti prescritti

Ai fini dell'attuazione dei comportamenti di cui sopra, SISSI definisce dei principi di attuazione dei comportamenti prescritti all'interno delle attività sensibili, come individuate nel paragrafo 6.2 della presente sezione, che devono trovare precisa attuazione nei protocolli, nelle procedure e nelle sottoprocedure di prevenzione.

I principi di attuazione dei comportamenti prescritti sono di seguito riportati:

(I) Rapporti con i rappresentanti della Pubblica Amministrazione

I rapporti con i rappresentanti della Pubblica Amministrazione nello svolgimento delle operazioni attinenti le attività sensibili, sono tenuti dall'Amministratore Unico oppure da un soggetto da questi delegato.

E' vietato a chiunque altro di intrattenere rapporti, per conto della Società, con esponenti della Pubblica Amministrazione.

(II) Rapporti con consulenti e collaboratori

Non vi deve essere identità di soggetti, all'interno della Società, tra chi richiede la consulenza e/o collaborazione, chi autorizza e chi esegue il pagamento. Ne consegue, in considerazione dell'organizzazione aziendale di SISSI, che gli incarichi di consulenza devono essere deliberati dall'Amministratore Unico o, se costituito, dal Comitato Esecutivo.

Consulenti e collaboratori devono essere scelti sulla base di precisi requisiti di onorabilità, professionalità e competenza ed in relazione alla loro reputazione e affidabilità.

I contratti con consulenti e collaboratori devono essere definiti per iscritto in tutte le loro condizioni e termini.

I compensi dei consulenti e collaboratori devono trovare adeguata giustificazione nell'incarico conferito e devono essere congrui, in considerazione delle prassi esistenti sul mercato e/o delle tariffe vigenti.

Nessun pagamento a consulenti e collaboratori può essere effettuato in contanti.

E' fatto divieto affidare ai consulenti e collaboratori qualsiasi attività che non rientri nel contratto di consulenza.

(III) Gestione delle erogazioni pubbliche

Per ogni contributo, finanziamento, sovvenzione ottenuti dallo Stato, dagli enti pubblici o dalla Unione Europea deve essere predisposto un apposito rendiconto che dia atto degli scopi per i quali l'erogazione pubblica è stata richiesta e concessa e della sua effettiva utilizzazione.

(IV) Rapporti con organi ispettivi

Nel caso di ispezioni giudiziarie, tributarie e amministrative (ad esempi relative al D. Lgs n. 81/2008, verifiche tributarie, INPS, NAS, ASL, ecc) i rapporti con gli organi ispettivi devono essere tenuti dal responsabile della funzione o da soggetto da questi delegato.

Il responsabile della funzione o il soggetto da questi delegato è tenuto a verificare che gli organi ispettivi redigano verbale delle operazioni compiute e richiederne una copia, in tutti i casi in cui ve ne sia il diritto; tale copia dovrà essere adeguatamente conservata. Nel caso in cui non fosse stato possibile ottenere il rilascio di una copia del verbale ispettivo, il responsabile della funzione o il soggetto da questi delegato a partecipare all'ispezione provvederà a redigere un verbale ad uso interno. Il personale della Società, nell'ambito delle proprie competenze, deve prestare piena collaborazione, nel rispetto della legge, allo svolgimento delle attività ispettive.

Il responsabile della funzione deve informare con una nota scritta l'Organismo di Vigilanza qualora, nel corso o all'esito della ispezione, dovessero emergere profili critici.

(V) Gestione del personale

Il delegato alla gestione del personale è tenuto a garantire l'applicazione di criteri di valutazione dei candidati che risponda alle esigenze di obiettività e trasparenza:

- a) l'assunzione dei candidati deve avvenire nel rigoroso rispetto delle procedure standard definite dall'azienda per la selezione del personale;
- b) l'esito del processo valutativo dei candidati sia formalizzato in apposita documentazione, accuratamente archiviata dal Responsabile competente secondo le prestabilite procedure interne.

6.6 Procedure di prevenzione

SISSI adotta un sistema di controlli interno diretto a prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione.

7 Reati societari

7.1 La tipologia dei reati societari (art. 25 ter del Decreto)

Per quanto concerne la presente Parte Speciale, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 25 ter del Decreto, che si possono raggruppare in 5 tipologie.

Falsità in comunicazioni, prospetti e relazioni

False comunicazioni sociali (artt. 2621 e 2622 c.c.)

*Qualora gli amministratori, i direttori generali, 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 appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino ad un anno e sei mesi.*

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti od amministrati dalla società per conto 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% o una variazione del patrimonio netto non superiore all'1%. La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla Società per conto di terzi.

Il reato previsto dall'art. 2621 cod. civ. (false comunicazioni sociali), come modificato dall'art. 1 del decreto legislativo 11 aprile 2002 n. 61, si distingue da quello di cui all'art. 2622 stesso codice (false comunicazioni sociali in danno dei soci o dei creditori), atteso che, nel primo, sono punite le false comunicazioni dirette ai soci o al pubblico, nel secondo, quelle che provocano una diminuzione patrimoniale per i soci o i creditori. Ne consegue che, mentre l'art. 2621 cod. civ. prevede un reato di pericolo (a tutela della regolarità dei bilanci e delle altre comunicazioni sociali, in quanto interesse della generalità), l'art. 2622 introduce nell'ordinamento un reato di danno a tutela degli interessi di soci e creditori.

Le relazioni

Il termine "relazione" viene usato nella disciplina civilistica delle società di capitali per indicare dei particolari rapporti informativi dei soggetti qualificati aventi la caratteristica della forma scritta ed obbligatori al ricorrere di situazioni normativamente stabilite.

Sono previste in particolare le seguenti relazioni:

- la relazione degli amministratori (art. 2428 c.c.) e quella dei sindaci (art. 2429 c.c.) che accompagnano il bilancio ordinario d'esercizio
- la relazione degli amministratori necessaria nel procedimento previsto per la distribuzione di acconti sui dividendi (art. 2433 bis, V comma c.c.)
- la relazione degli amministratori con cui si deve illustrare la proposta di aumento di capitale con esclusione o limitazione del diritto di opzione (art. 2441, VI comma c.c.)

Il precedente elenco non è fine a se stesso, bensì volto a sottolineare come la lettura del termine "relazioni" debba essere restrittiva: in sostanza esso sta ad indicare le sole "relazioni tipiche" (id est: i rapporti scritti relativi ad attività sociali espressamente previsti dalla legge).

I bilanci

Quanto alla categoria dei "bilanci", essa è certamente comprensiva del bilancio d'esercizio o ordinario (artt. 2423 e seg. c.c.) "inteso come strumento di informazione patrimoniale, finanziaria ed economica dell'impresa in funzionamento, cioè di un'impresa caratterizzata dalla continuità operativa".

Unitamente ai suddetti si devono considerare in linea generale anche il bilancio consolidato (ossia il documento contabile destinato a fornire un quadro della situazione economica e finanziaria del gruppo unitamente considerato) e fungere da possibile contenitore di falsità espresse dall'art. 2621 n. 1 c.c. e tutti i bilanci la cui natura è straordinaria, tra cui possono in genere essere compresi quei prospetti contabili che servono ad esporre la situazione patrimoniale della società in occasione di eventi diversi dalla chiusura del normale esercizio sociale od in occasione di particolari vicende giudiziarie o amministrative. Sono considerati bilanci straordinari ad esempio il prospetto contabile (ex art. 2433 bis, V comma c.c.) richiesto ai fini della distribuzione di acconti sui dividendi; il bilancio finale di liquidazione di cui agli artt. 2311 e 2453 c.c., la situazione patrimoniale redatta con l'osservanza della normativa sul bilancio d'esercizio (art. 2501 ter, I comma c.c.) che accompagna il progetto di fusione (art. 2501, III comma) o di scissione (art. 2504 novies c.c.); il bilancio che deve essere depositato unitamente all'istanza di fallimento della società (art. 14 L. fall.).

Le altre comunicazioni sociali

E' bene sottolineare che in linea di principio al fine di individuare quali siano da considerarsi comunicazioni sociali si devono tenere presenti i seguenti requisiti: il primo relativo al soggetto dell'atto, cioè "l'ufficialità"; il secondo determinato dalla sua relazione con l'oggetto, ossia "l'inerenza all'oggetto sociale"; il terzo riguarda i suoi destinatari: "la direzionalità pubblica". In merito al primo, la dottrina ed una giurisprudenza ormai consolidata sono concordi nel ritenere requisito imprescindibile della comunicazione, penalmente rilevante, il carattere dell'ufficialità integrato ogni qualvolta la stessa sia emessa dai soggetti qualificati nell'esercizio ed in virtù delle funzioni specifiche loro attribuite nell'ambito di una società già costituita o costituenda. Di conseguenza le cosiddette informazioni confidenziali o private, la cui falsità non potrà integrare gli estremi del delitto in esame, sono prive del requisito dell'ufficialità ma la falsità potrà, nel concorso dei relativi estremi, essere causa di responsabilità penale a titolo di truffa o di agiotaggio societario.

Infine, con il terzo requisito si vuole attribuire rilevanza penale soltanto alle informazioni, ufficiali ed inerenti all'oggetto sociale, che siano potenzialmente riferite ad una pluralità di destinatari; ossia il carattere della direzionalità pubblica sarebbe "la rilevanza esterna" che si concretizzerebbe ogni qualvolta la comunicazione è destinata ad un numero indeterminato di soggetti ovvero ai soci, creditori sociali e terzi (potenzialmente soci o creditori) tutelati non come singoli ma come "categorie aperte".

In merito alla forma, anche se teoricamente potrebbe rivelarsi contestabile, è opportuno segnalare che anche solamente la forma verbale potrebbe configurare un'ipotesi di comunicazione falsa da tenere presente. Ad esempio le false dichiarazioni rese dagli amministratori o dai sindaci all'assemblea dei soci o degli obbligazionisti, o dai promotori dell'assemblea dei sottoscrittori.

Non saranno considerate propriamente "sociali" le comunicazioni che i singoli membri di organi collegiali (Assemblea dei soci e collegio sindacale) attuano nei confronti degli organi stessi, oppure quelle rese dagli amministratori all'organo di controllo interno.

Il falso nelle scritture contabili e nei libri sociali

E' opportuno sottolineare che, in linea generale, anche eventuali alterazioni dei libri sociali, la cui caratteristica è quella di essere istituiti come un "mezzo di informazione per i soci e gli eventuali terzi", possono concretizzare delle violazioni di falso ai sensi dei reati di cui sopra.

Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.)

Il reato consiste in **false attestazioni** od occultamento di informazioni **da parte dei responsabili della revisione**, concernenti la situazione economica, patrimoniale o finanziaria della società, al fine di conseguire un ingiusto profitto per sé o per altri. La sanzione è più grave se la condotta ha provocato un danno patrimoniale ai destinatari delle comunicazioni.

Soggetti attivi sono responsabili della società di revisione (reato proprio), ma i componenti degli organi di amministrazione e di controllo SISSI e i suoi dipendenti possono essere coinvolti a titolo di concorso di reato.

Tutela penale del capitale sociale

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

La condotta tipica consiste nella **restituzione dei conferimenti ai soci** o la liberazione degli stessi dall'obbligo di eseguirli, in modo palese o simulato, **fuori dei casi di legittima riduzione del capitale sociale**.

In merito al presente reato, soggetti attivi sono gli amministratori (reato proprio) ma vi è la possibilità del concorso dei soci¹⁴, i quali possono aver contribuito con un'attività di istigazione, di determinazione o di ausilio nei confronti degli amministratori stessi.

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

La condotta criminosa di questo reato, di natura contravvenzionale, consiste nel **ripartire gli utili** o acconti sugli utili **non effettivamente conseguiti** o destinati per legge a riserva, **ovvero ripartire riserve**, anche non costituite con utili, che per legge non possono essere distribuite.

La ricostituzione degli utili o delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Anche in questo caso soggetti attivi del reato sono gli amministratori (reato proprio).

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

Il perfezionamento di questo reato si ha con **l'acquisto o la sottoscrizione di azioni o quote sociali della società controllante che cagioni una lesione all'integrità del capitale sociale** e delle riserve non distribuibili per legge.

¹⁴ Secondo le regole generali di cui agli artt. 110 e seguenti c.p.

Tale reato si estingue se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione a cui è stata posta in essere la condotta.

Soggetti attivi del reato sono gli amministratori della società controllata, nel caso in cui le operazioni illecite fossero effettuate sulle azioni della società controllante, mentre una responsabilità degli amministratori della società controllante è configurabile solo a titolo di concorso. Anche i soci possono rispondere allo stesso titolo.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Il reato si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di **riduzioni del capitale sociale** o fusioni con altra società o scissioni, **che cagionino danno ai creditori**.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono gli amministratori.

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

Il reato è integrato dalle seguenti condotte:

- fittizia formazione o aumento del capitale sociale mediante **attribuzione di azioni** o quote in misura complessivamente **superiore all'ammontare del capitale sociale**;
- **sottoscrizione reciproca di azioni** o quote;
- **sopravalutazione rilevante dei conferimenti di beni in natura**, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti. In questo caso, però, non è incriminato l'omesso controllo ed eventuale revisione da parte di amministratori e sindaci della valutazione dei conferimenti in natura (ai sensi dell'art. 2343, III comma c.c.) contenuta nella relazione di stima redatta dall'esperto nominato dal Tribunale.

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

Il reato si perfeziona attraverso la **ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali** o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Il reato si estingue con il risarcimento del danno ai creditori prima del giudizio.

Soggetti attivi del reato sono unicamente gli amministratori.

Tutela penale del regolare funzionamento della società

Impedito controllo (art. 2625 c.c.)

La fattispecie si realizza con l'**impedire o l'ostacolare**, attraverso occultamento di documenti o altri idonei artifici, **lo svolgimento delle attività di controllo o di revisione** legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione.

Soggetti attivi del reato sono gli amministratori.

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

La condotta consiste nel fatto che si **determini con atti simulati o con frode la maggioranza in assemblea** (reato di evento), **al fine di conseguire**, per sé o per altri, **un ingiusto profitto** (dolo specifico).

Tale reato è considerato come un reato comune per cui può essere commesso da chiunque, compresi soggetti estranei alla società.

Tutela penale contro le frodi

Aggiotaggio (art. 2637 c.c.)

Il reato si perfeziona con la diffusione di notizie false ovvero si realizzino operazioni simulate o altri **artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari**, ovvero a incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari. Anche questo reato è un reato comune e quindi può essere commesso da chiunque.

Tutela penale delle funzioni di vigilanza

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

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

1 – il reato si realizza attraverso l'esposizione delle comunicazioni alle autorità di vigilanza previste dalla legge, con lo scopo di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, o oggetto di valutazioni sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima (I comma).

2 – il reato si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente ed in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza (II comma).

E' bene precisare che:

- la prima ipotesi si basa su una condotta di falsità che persegue il fine specifico di ostacolare le funzioni di vigilanza (dolo specifico)
- la seconda ipotesi delinea un reato di evento (ostacolo all'esercizio delle funzioni di vigilanza) a forma libera, realizzabile, cioè con qualsiasi modalità di condotta, inclusi i comportamenti omissivi il cui elemento soggettivo è costituito dal dolo generico.

Soggetti attivi di entrambe le ipotesi di reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

7.2 Aree di attività a rischio

Relativamente a ciascuna delle tipologie di reato sopra descritte si può delineare una specifica area astrattamente a rischio. A seguito del processo di autovalutazione condotta internamente a SISSI sono state individuate le seguenti attività a rischio:

ATTIVITA'	RESPONSABILITA' INTERNA SISSI	SISTEMI DI CONTROLLO UTILIZZATI
Gestione del piano dei conti e della contabilità generale, (inserimento, variazione o cancellazione dei dati di contabilità generale).	Responsabile Amministrativo	Procedure contabili All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI PG per la FORMAZIONE del BILANCIO e GESTIONE delle COMUNICAZIONI SOCIALI Codice Etico
Raccolta, aggregazione e valutazione dei dati contabili necessari alla predisposizione della bozza di bilancio (societario e consolidato).	Responsabile Amministrativo	Procedure contabili All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI Codice Etico
Redazione delle relazioni allegare ai prospetti economici, finanziari e patrimoniali di bilancio, nonché predisposizione di prospetti informativi informali.	Consulente esterno	Procedure contabili All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI Codice Etico
Approvazione del bilancio e definizione degli utili da distribuire.	Legale Rappresentante	Codice Etico All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI
Predisposizione di dichiarazioni dei redditi e dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione dei tributi in genere	Consulente esterno	Codice Etico All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI
Comunicazione, svolgimento, verbalizzazione e archiviazione delle assemblee	Responsabile Amministrativo	Codice Etico All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI
Operazioni straordinarie	Legale Rappresentante	Codice Etico
Gestione dei rapporti con i Soci conferenti Capitale Sociale	Responsabile Amministrativo	Codice Etico All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI
Produzione reportistica da presentare all'Assemblea	Responsabile Amministrativo	Codice Etico All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI
Gestione della sicurezza dei sistemi informatici	Responsabile Amministrativo	Codice Etico Blocchi di profilazione effettuati dal consulente informatico
Gestione dei rapporti con Banche / Istituti di credito	Responsabile Amministrativo	Codice Etico All. 2, 3, 5 e TABELLA ACQUISTO BENI E SERVIZI

In relazione ai reati societari, le aree di attività ritenute più specificatamente a rischio devono essere individuate come segue:

- la predisposizione di comunicazioni dirette ai soci o al pubblico in generale in merito alla situazione economica, patrimoniale e finanziaria della Società nel suo insieme (redazione del bilancio d'esercizio, della relazione sulla gestione e di altre comunicazioni sociali);
- la divulgazione verso l'esterno di dati o notizie anche ulteriori a quelle sopra indicate, inerenti la Società;
- operazioni societarie che possono incidere sull'integrità del capitale sociale;
- le attività di controllo legalmente attribuite ai Soci e agli altri organi sociali preposti al controllo e alla società di revisione.

7.3 Destinatari della parte speciale

Destinatari della presente Parte Speciale sono i soggetti di volta in volta individuati dalla fattispecie incriminatrice (amministratori, direttori generali, sindaci, dipendenti, liquidatori, ecc) "soggetti apicali" di SISSI, nonché i dipendenti sottoposti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, questi soggetti saranno di seguito denominati "Destinatari".

In merito agli amministratori, al dirigente preposto, ai direttori generali, ai sindaci e ai liquidatori, la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto". Ai sensi dell'art. 2639 c.c., infatti, dei reati societari previsti dal codice civile risponde sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Obiettivo della presente Parte Speciale è che al fine di impedire il verificarsi dei reati previsti nel Decreto:

- tutti i Destinatari come sopra descritti siano precisamente consapevoli della valenza dei comportamenti censurati e
- adottino quindi regole di condotta conformi a quanto prescritto dalla stessa.

7.4 Principi generali di comportamento

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

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25 ter del Decreto)
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

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

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
2. tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure aziendali interne, al fine di garantire la tutela del patrimonio degli investitori, ponendo la massima attenzione e accuratezza nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni relative ai prodotti finanziari e ai loro emittenti;
3. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e 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;
4. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

5. osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando rigorosamente di porre in essere comportamenti idonei a provocare una sensibile alterazione in relazione alla concreta situazione del mercato;
6. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

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

◆ con riferimento al precedente punto 1:

1.a. rappresentare o trasmettere per l'elaborazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi, o comunque, non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della Società;

1.b. omettere la comunicazione di dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società e del gruppo di appartenenza;

◆ con riferimento al precedente punto 2:

2.a. alterare i dati e le informazioni destinati alla predisposizione del prospetto;

2.b. illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione finanziaria, economica e patrimoniale della Società e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi diritti;

2.c. inficiare la comprensibilità del prospetto accrescendo oltremisura la massa dei dati, delle informazioni e delle parti descrittive contenute nel prospetto rispetto a quanto richiesto dalle effettive esigenze informative dell'investitore;

◆ con riferimento al precedente punto 3:

3.a. restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale, in qualsiasi forma non specificamente compresa fra quelle di seguito descritte;

3.b. ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;

3.c. acquistare o sottoscrivere azioni della società fuori dai casi previsti dalla legge;

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

3.e. procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni o quote per un valore inferiore al loro valore nominale in sede di costituzione di società o di aumento del capitale sociale;

3.f. distrarre i beni sociali, in sede di liquidazione della Società, dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli;

◆ con riferimento al precedente punto 4:

4.a. porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento dell'attività di controllo o di revisione della gestione;

4.b. determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

◆ con riferimento al precedente punto 5:

5.a. pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio aventi ad oggetto strumenti finanziari quotati o non quotati e idonei ad alterarne sensibilmente il prezzo (price sensitivity);

5.b. pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio idonei a diffondere sfiducia nel pubblico di banche o gruppi bancari, alterandone l'immagine di stabilità e liquidità;

◆ con riferimento al precedente punto 6:

6.a. omettere di effettuare, con la dovuta qualità e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa di settore nei confronti delle Autorità di Vigilanza cui è soggetta

l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;

6.b. esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti, in relazione alle condizioni economiche, patrimoniali o finanziarie della Società;

6.c. porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti.

7.5 Principi di attuazione dei comportamenti prescritti

Vengono di seguito descritti i principi e le modalità di attuazione dei comportamenti di cui sopra in relazione alle diverse tipologie dei reati societari, che devono trovare specifica attuazione nelle procedure di prevenzione.

Le regole generali di organizzazione sono di seguito riportate:

(I) Redazione di bilanci, scritture contabili, relazioni ed altri documenti di impresa

Le operazioni di rilevazione e registrazione delle attività di impresa devono essere effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza.

Tutti i dati e le informazioni che servono alla redazioni dei bilanci (bilancio d'esercizio) e degli altri documenti contabili della Società devono essere chiari, completi e rappresentare in modo veritiero la situazione economica, finanziaria e patrimoniale della Società.

I dati e le informazioni sono raccolti tempestivamente, sotto la supervisione dell' Amministratore Unico, ed elaborati da soggetti da questo delegati ai fini della predisposizione della bozza di bilancio. A richiesta, insieme ai dati e alle informazioni devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni.

La redazione del bilancio d'esercizio deve essere effettuata sulla base della prassi consolidata e, periodicamente. Eventuali variazioni non giustificate dei principi contabili stabiliti dalle procedure, devono essere tempestivamente segnalate all'Organismo di Vigilanza.

(II) Tutela del patrimonio sociale

Tutte le operazioni relative alla destinazione degli utili, alla costituzione di società, all'acquisto e cessione di partecipazioni, alle fusioni e scissioni nonché tutte le operazioni che possono ledere l'integrità del patrimonio sociale devono essere effettuate nel rispetto dello Statuto, del Codice Etico e delle procedure aziendali a tale scopo predisposte.

(III) Rapporti con i Sindaci (non applicabile)

(IV) Rapporti con consulenti e collaboratori

Si applicano le regole generali indicate nella Parte Speciale di cui al capitolo 6 (Rapporti con consulenti e collaboratori) del presente Modello.

(V) Interessi degli amministratori nelle operazioni della Società

Nel rispetto della norma di cui all'art. 2391 cod.civ., gli amministratori devono dare notizia agli altri Amministratori di ogni interesse che essi, per conto proprio o di terzi (incluso ogni soggetto con cui gli amministratori intrattengano, direttamente o indirettamente, relazioni economiche o di cui siano dipendenti o amministratori), abbiano in una determinata operazione della Società, precisandone la natura, i termini, l'origine e la portata. In conformità a quanto previsto nel Codice Etico della Società, gli amministratori devono astenersi dal votare tale operazione o transazione.

Le segnalazioni concernenti gli interessi degli amministratori nelle operazioni della Società devono essere inviate all'Organismo di Vigilanza, che ne cura l'archiviazione e l'aggiornamento.

7.6 Procedure di prevenzione

La Società adotta un sistema di controlli interno volto a prevenire la commissione dei reati societari.

Il sistema si compone di procedure e protocolli che regolano le fasi di formazione e attuazione delle decisioni della Società nell'ambito delle attività sensibili. Le procedure si aggiungono alle prassi applicative diffuse all'interno della Società.

La prevenzione dei reati sopra descritti avviene tramite applicazione delle normali procedure previste per la certificazione e per la gestione societaria

Per la corretta gestione delle procedure necessarie alla formazione del bilancio viene incaricato un consulente esterno (commercialista) il quale assume uno specifico impegno di monitoraggio, supervisione e controllo della correttezza delle registrazioni contabili.

Ad ulteriore garanzia della commissione dei reati l'OdV dovrà essere notiziato da parte dell'Amministratore Unico nel caso di operazioni straordinarie.

8.1 La fattispecie di reato

Per quanto concerne la presente Parte Speciale, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 24 bis del Decreto.

Documenti informatici (art. 491-*bis* cod. penale).

"Se alcune delle falsità 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".

Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* cod. 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".

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* cod. 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. 617*quater*".*

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinqües* cod. 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".

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* cod. 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".

Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. 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*."*

Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* cod. 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 a quattro anni e si procede d'ufficio."

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-*ter* cod. 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."

Danneggiamento di sistemi informatici e telematici (art. 635-*quater* cod. 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"

Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635- *quinquies* cod. 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"

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* cod. 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".

8.2 Aree di attività a rischio

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall'art. 24- *bis* del D.Lgs. 231/2001, sono relative alla gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

ATTIVITA'	RESPONSABILITA' INTERNA SISSI	SISTEMI DI CONTROLLO UTILIZZATI
Gestione dei sistemi informativi e trattamento illecito delle informazioni	Responsabile Amministrativo	Codice Etico Blocchi di profilazione effettuati dal consulente informatico DPS privacy
Gestione del profilo utente e del processo di autenticazione	Legale Rappresentante	Codice Etico Blocchi di profilazione effettuati dal consulente informatico DPS privacy
Gestione e protezione della postazione di lavoro	Legale Rappresentante	Codice Etico Blocchi di profilazione effettuati dal consulente informatico DPS privacy
Utilizzo di firma elettronica	Legale Rappresentante	Codice Etico
Predisposizione ed invio telematico di scritture private e/o attestazioni e/o dichiarazioni sostitutive di certif. o atto di notorietà DPR 445/2000	Consulente esterno	Codice Etico
Gestione degli output di sistema e dei sistemi di memorizzazione	Consulente esterno Responsabile Amministrativo	Codice Etico Blocchi di profilazione effettuati dal consulente informatico DPS privacy
Gestione e protezione delle reti	Responsabile Amministrativo	Codice Etico Blocchi di profilazione effettuati dal consulente informatico DPS privacy

Con specifico riguardo alle problematiche connesse al rischio informatico, SISSI, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e (ii) la garanzia della massima continuità del servizio.

8.3 Destinatari della Parte Speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dai dirigenti e dai dipendenti "esponenti aziendali" di SISSI nelle aree di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella Parte Generale (qui di seguito tutti denominati "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

8.4 Principi generali di comportamento

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che SISSI si pone sono i seguenti:

- **Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- **Integrità:** garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- **Disponibilità:** garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di SISSI (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) 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. 24-*bis* del D.Lgs. 231/2001);

- violare i principi e le procedure aziendali previste nella presente parte speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- 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;
- k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;
5. evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;

6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi;
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

8.5 Procedure di prevenzione

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici 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: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) 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.

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

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 all'Amministratore Unico secondo le modalità previste nella Parte Generale del presente Modello.

9.1 La fattispecie di reato

La presente sezione della Parte Speciale si riferisce ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, richiamati dall'art.25-septies del Decreto e di seguito riportati.

A differenza delle altre ipotesi di reato presupposto previste nel Decreto che richiedono la sussistenza del dolo (coscienza e volontarietà dell'azione criminosa), i delitti di cui alla presente Parte Speciale sono puniti a titolo di colpa.

Omicidio colposo (art. 589 c.p.)

E' punita la condotta di chiunque cagiona per colpa la morte di una persona con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Lesioni colpose gravi o gravissime (art. 590 c.p.)

E' punita la condotta di chiunque cagioni ad altri per colpa una lesione personale grave o gravissima con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

La lesione è grave se:

1. dal fatto deriva una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai 40 giorni;
2. il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione è gravissima se dal fatto deriva:

1. una malattia certamente o probabilmente insanabile;
2. la perdita di un senso;
3. la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;
4. la deformazione ovvero lo sfregio permanente del viso.

9.2 Aree di attività a rischio

L'attività che la Società ha individuato al proprio interno come sensibile, nell'ambito dei reati e dei corrispondenti illeciti amministrativi, di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro è:

ATTIVITA'	RESPONSABILITA' INTERNA SISSI	SISTEMI DI CONTROLLO UTILIZZATI
Nomina del RSPP	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Acquisizione documentazione per le Certificazioni obbligatorie	Responsabile Amministrativo	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Valutazione dei Rischi e elaborazione del relativo documento	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Elaborazione delle Procedure in materia di sicurezza, prevenzione incendi, primo soccorso e verifiche periodiche delle stesse	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Individuazione ed elaborazione delle Misure preventive e protettive e dei DPI	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Individuazione fattori a rischio	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Informazione ai lavoratori sui rischi per la salute e misure di prevenzione e protezione adottate	RSPP	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Assegnazione mansioni	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Conservazione ed aggiornamento Registro Infortuni	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Informazione e Formazione dei lavoratori	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1

ATTIVITA'	RESPONSABILITA' INTERNA SISSI	SISTEMI DI CONTROLLO UTILIZZATI
Invio informazioni al RSPP, al datore di lavoro e all'Organismo di Vigilanza	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Ispezioni per prevenzione incendi	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Programmazione riunioni periodiche sulla sicurezza	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1
Vigilanza sulle procedure adottate e delle istruzioni date ai lavoratori	Legale Rappresentante	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 e s.m.i. All. 1

Eventuali integrazioni della suddetta area di attività a rischio potranno essere disposte dall'Amministratore Unico di SISSI Srl di concerto con l'Organismo di Vigilanza, a cui è dato mandato di definire gli opportuni provvedimenti operativi.

9.3 Destinatari della Parte Speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dirigenti, RSPP e dipendenti "esponenti aziendali" di SISSI nell'area di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella parte Generale (di seguito tutti denominati "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati adottino regole di condotta conformi a quanto prescritto dalla stessa, al fini di impedire il verificarsi dei reati previsti nel Decreto.

9.4 Principi generali di comportamento

Nello svolgimento delle attività, tutti i Destinatari del Modello sono tenuti ad osservare i principi generali di comportamento che la Società ha individuato in conformità anche a quanto previsto dal Codice Etico e alle regole dettate dalla normativa in materia di tutela dell'igiene, della salute e per la sicurezza dei lavoratori.

In particolare la Società adotta le seguenti misure generali:

1. attenta valutazione dei rischi e completa trasposizione degli stessi nel Documento di Valutazione dei rischi;
2. eliminazione dei rischi per la salute e la sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non possibile, loro riduzione al minimo;
3. riduzione dei rischi alla fonte;
4. programmazione della prevenzione mirando ad un complesso che integra in modo coerente nella prevenzione le condizioni tecniche produttive ed organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro;
5. sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
6. rispetto dei principi ergonomici nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, anche per attenuare il lavoro monotono e quello ripetitivo;

7. priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;
8. limitazione al minimo dei lavoratori che sono, o che possono essere esposti al rischio;
9. utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di lavoro;
10. controllo sanitario dei lavoratori in funzione dei rischi specifici;
11. allontanamento del lavoratore dall'esposizione a rischio, per motivi sanitari inerenti la sua persona;
12. misure igieniche;
13. misure di protezione collettiva e individuale;
14. misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;
15. uso di segnali di avvertimento e di sicurezza,
16. regolare manutenzione di ambienti, attrezzature, macchine ed impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti;
17. informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro;
18. istruzioni adeguate ai lavoratori.

9.5 Procedure di prevenzione

La Società ha implementato un sistema di controlli volto alla creazione di un canale informativo nei confronti dell'organismo di Vigilanza al fine di prevenire la commissione dei reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

10.1 La fattispecie di reato

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES, D.LGS. 231/01)

Si riporta di seguito una breve descrizione dei reati contemplata dall'art. 25-novies del Decreto e che possono riguardare potenzialmente l'Ente.

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis);
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1);
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941);
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941);

10.2 Aree di attività a rischio

I reati sopra indicati sono caratterizzati dalla previsione che l'attività illecita abbia ad oggetto la violazione del diritto d'autore ad opera di un soggetto operante all'interno dell'Ente.

In particolare, si considerano a rischio tutte le aree di SSSI che potenzialmente nell'esercizio delle proprie funzioni potrebbero violare il diritto di autore di un altro soggetto, legalmente tutelato. In particolare, possiamo individuare un maggior rischio in quelle aree, come le Unità Operative Gestione, Amministrazione, Segreteria, Qualità e Comunicazione che utilizzano sistemi informatici, i quali, generalmente sono protetti da un copyright e poiché la loro attività si esplica proprio attraverso la stipula di accordi con soggetti terzi che potrebbero prevedere l'utilizzo di documenti protetti dal diritto d'autore. Inoltre, si sottolinea, come anche nell'erogazione dei servizi agli utenti la società è a rischio di commissione reato.

10.3 Destinatari della Parte Speciale

Questa Parte Speciale si riferisce a comportamenti posti in essere da chiunque operando nelle aree di attività a rischio, violi il diritto d'autore legalmente tutelato esponendo SSSI ad un rischio legale, oltre che reputazionale.

10.4 Principi generali di comportamento

Nell'espletamento della propria attività, tutti i dipendenti/collaboratori di SISSI sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati del Modello e, in particolare, dal Codice Etico.

È inoltre necessario:

- che sia garantito il rispetto del Codice Etico;
- che tutte le attività svolte siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- che sia rispettato il principio di separazione dei ruoli e responsabilità nelle fasi dei processi Aziendali.

A tutti i dipendenti/collaboratori dell'Ente è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione dei comportamenti tali da integrare le fattispecie di delitti relativi al diritto d'autore sopra richiamati;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

10.5 Procedure di prevenzione

L'Ente ha implementato un sistema di controlli volto alla creazione di un canale informativo nei confronti dell'Organismo di Vigilanza al fine di prevenire la commissione dei reati commessi con violazione delle norme a tutela dei diritti d'autore.

Per la prevenzione dei reati previsti nella presente Parte Speciale, l'Organismo di Vigilanza dovrà effettuare controlli nei confronti dei Destinatari della presente Parte Speciale, al fine di verificare l'osservanza delle prescrizioni ivi previste.

ATTIVITA'	RESPONSABILITA' SISSI	SISTEMI DI CONTROLLO UTILIZZATI
Utilizzo di materiale con copyright	Responsabile sistemi qualità e responsabile Amministrativo	Codice Etico

11 Attività strumentali alla commissione dei reati

11.1 Attività strumentali alla commissione dei reati

La Società adotta un sistema di controlli interni con lo scopo di monitorare tutte quelle attività che potrebbero costituire un supporto per la commissione dei reati nei processi aziendali in cui si intrattengono relazioni con la Pubblica Amministrazione. In particolare la seguente tabella elenca i processi sensibili ed i relativi standard di controllo organizzativo su cui è stata condotta l'analisi.

ATTIVITA'	RESPONSABILITA' SSISS	SISTEMI DI CONTROLLO UTILIZZATI
Selezione ed assunzione del personale	a. Responsabile Amministrativo.	Codice Etico
Gestione di omaggi	a. Responsabile Amministrativo	Codice Etico Divieto di acquisto di beni al di sopra dell'importo di € 50,00
Spese di rappresentanza	Responsabile Amministrativo	Codice Etico Divieto di acquisto di beni al di sopra dell'importo di € 50,00 TABELLA ACQUISTO DI BENI E SERVIZI
Incarichi a professionisti	RESPONSABILE AMMINISTRATIVO	Codice Etico Divieto di acquisto di servizi al di sopra dell'importo di € 5000,00 TABELLA ACQUISTO DI BENI E SERVIZI
Approvvigionamento di beni e servizi	RESPONSABILE AMMINISTRATIVO	Codice Etico TABELLA ACQUISTO DI BENI E SERVIZI

11.2 Procedure di prevenzione

Le procedure di prevenzione, poste a presidio delle attività sensibili indicate nel precedente paragrafo, sono adottate nelle seguenti aree: Acquisti di beni e servizi, incarichi professionali a terzi e gestione del personale.

AII. 1

PG RAPPORTI CON LA PA IN MATERIA DI LAVORO, PREVIDENZA, SICUREZZA E FISCALE

In caso di Verifiche in materia di previdenza e sicurezza, accertamenti o indagini fiscali e/o altri funzionari di enti verificatori, i rapporti con i soggetti preposti ai controlli, dovranno essere tenuti dall'amministratore Unico

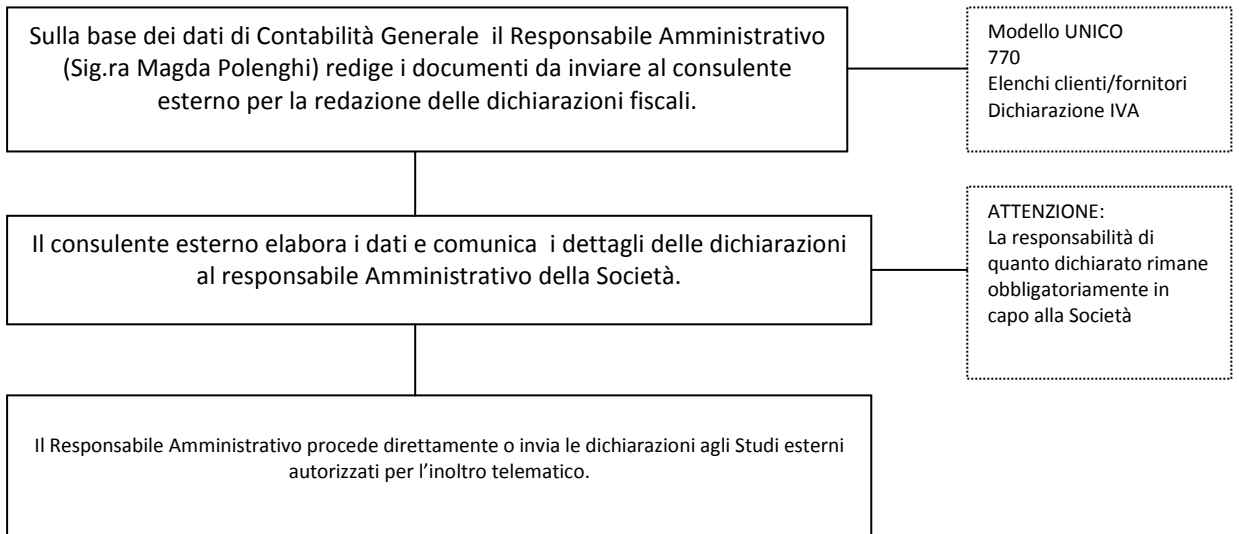
L'amministratore dovrà essere presente all'inizio delle operazioni di verifica giornaliera e alla chiusura delle stesse, essi stessi sono gli unici soggetti autorizzati alla custodia della documentazione oggetto di controllo.

Dovranno essere redatti un verbale di apertura che si accompagna al verbale dell'autorità verificatrice e che indicherà le figure preposte ed un verbale di chiusura che sintetizza l'oggetto della verifica e l'esito della stessa. Entrambi i verbali dovranno essere portati a conoscenza alla prima riunione dell'assemblea.

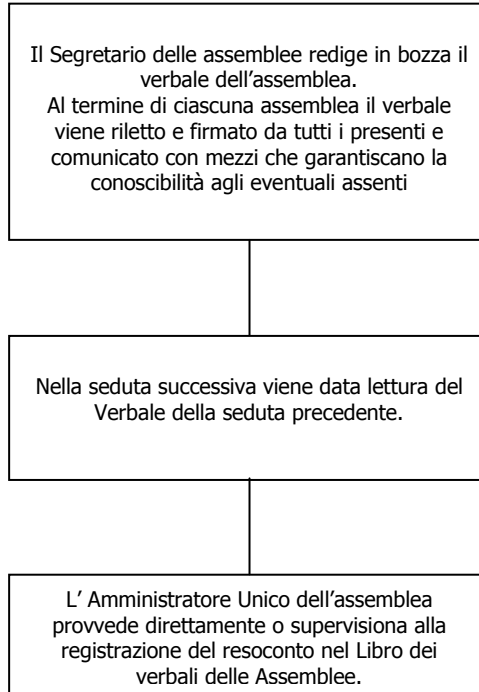
PG PER LA GESTIONE DELLA CASSA

- 1.** SISSI non usa contanti per le operazioni correnti salvo che per le seguenti:
 - SPESE POSTALI
 - VERSAMENTI IN C/C DELLE SOMME DI CUI AL PUNTO 2
 - CARBURANTE
 - CANCELLERIA
 - RIMBORSI SPESE RISTORANTE
 - RIMBORSI SPESE DOCUMENTATE (PARCHEGGI AUTO, ECC.)
 - RIMBORSI INDENNITA' CHILOMETRICA (UTILIZZO AUTO PROPRIA)
- 2.** Sissi effettua incassi per contanti per cifre al di sotto di € 500,00 per ciascuna commessa.
- 3.** La cassa è affidata alla gestione della Sig.ra Magda Polenghi che, da sola può usare il denaro della cassa e compiere le necessarie registrazioni contabili.

All. 3
PG PER ADEMPIMENTI FISCALI



All.4
PG GESTIONE LIBRI SOCIALI: Verbalizzazione delle Delibere



PG per la FORMAZIONE del BILANCIO per la REGISTRAZIONE DEI DATI FINANZIARI e GESTIONE delle COMUNICAZIONI SOCIALI**Formazione del Bilancio**

- La Società prevede con atto formale e rintracciabile il conferimento di un incarico ad un professionista (Studio di Commercialisti) dell'incarico di registrazione dei dati contabili in corso d'anno.
- Il conferimento dell'incarico prevede una specifica responsabilità del commercialista per mancata segnalazione di elementi sospetti che possano far ritenere la commissione di uno dei reati previsti dal D.Lgs 231/01 fermo restando che il consulente potrà valutare la necessità delle predette segnalazioni unicamente in relazione alle informazioni ricevute e senza onere di verifica e tracciamento di ciascuna operazione contabile.
- La Società e' dotata di un sistema software di registrazione dei dati contabili che permetta la rintracciabilità del dato stesso. Solo la Sig.ra Polenghi è delegata a registrare i dati contabili relativi alle operazioni quotidiane.
- La Società si dota di un sistema che preveda altresì la tracciatura dei singoli passaggi qualora le informazioni vengano trasferite all'esterno dell'impresa.
- Le operazioni di assestamento di Bilancio che intercorrono tra la fase di registrazione contabile, la redazione del Bilancio verranno condotte in modo che ciascun passaggio sia tracciabile (fax, PEC, consegna della documentazione con controfirma di attestazione di ricezione e dettaglio analitico del materiale consegnato).

Gestione delle Comunicazioni Sociali

- La Società prevede che le Comunicazioni Sociali formali o informali verranno redatte, tracciate e organizzate dal professionista incaricato (es. Reportistica infrannuale, ecc) di concerto con l'Amministratore Unico.
- Tutte le comunicazioni sociali verranno effettuate con strumenti tracciabili (fax, PEC, consegna della documentazione con controfirma di attestazione di ricezione e dettaglio analitico del materiale consegnato)

Note

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale devono essere rispettate le regole e i principi generali di comportamento previsti nel Codice Etico ed in particolare gli Organi Societari, e i dipendenti e collaboratori nella misura necessaria alle funzioni dagli stessi svolte, devono in generale conoscere e rispettare le norme inerenti il sistema amministrativo, contabile e finanziario della Società.

TABELLA ACQUISTO DI BENI E SERVIZI

ATTIVITA'	AZIONI	RESPONSABILITA'	POTERE di FIRMA
Acquisto di beni / servizi di valore > 5.000,00 €	Il Responsabile Amministrativo valuta l'opportunità di effettuare l'acquisto e si confronta con l'Amministratore Unico che autorizza l'acquisto.	Responsabile Amministrativo Amministratore Unico	Amministratore Unico
Acquisto di beni / servizi di valore < a 5.000,00 € (e > a 10.000,00 €)	Il Responsabile Amministrativo valuta l'opportunità di effettuare l'acquisto e vaglia i preventivi predisposti. Il Responsabile Amministrativo propone le 3 offerte migliori all'Amministratore Unico che decide l'acquisto e delega i poteri necessari in forma scritta.	Responsabile Amministrativo Amministratore Unico	Amministratore Unico
Acquisto di beni / servizi di valore < a 10.000,00 €	Il Responsabile Amministrativo valuta l'opportunità di effettuare l'acquisto e vaglia i preventivi predisposti. Il Responsabile Amministrativo propone le 3 offerte migliori all'Amministratore Unico che relaziona l'assemblea che, a sua volta, decide l'investimento	Responsabile Amministrativo Amministratore Unico Assemblea	Responsabile Amministrativo Amministratore Unico