

## **Gruppo Helvetia Italia**

### **Documento illustrativo del Modello di organizzazione, gestione e controllo**

**Ai sensi del  
Decreto Legislativo  
n. 231 dell'8 giugno 2001**

**Approvato da:**

- Rappresentante Generale (per la Capogruppo)
- Consiglio di Amministrazione (per le Società del Gruppo)

**Data approvazione: 16 aprile 2010**

## Indice

<b>Definizioni.....</b>	<b>4</b>
<b>Parte Generale .....</b>	<b>5</b>
<b>1. Decreto legislativo 8 giugno 2001 n. 231 e successive integrazioni e modificazioni .....</b>	<b>5</b>
1.1 La disciplina della responsabilità amministrativa.....	5
1.2 I reati presupposto.....	5
1.3 Elementi chiave del Decreto.....	8
1.4 Autori del reato .....	8
1.5 Natura della responsabilità .....	8
1.6 Le sanzioni previste.....	9
1.7 La responsabilità della società .....	10
1.8 Soggetti in posizione apicale.....	10
1.9 Soggetti sottoposti a direzione o vigilanza del soggetto apicale .....	10
<b>2. Attività e organizzazione.....</b>	<b>12</b>
2.1 Aspetti organizzativi.....	12
2.2 Governance e sistema di controllo interno .....	13
2.3 Valori di riferimento e normativa interna.....	13
<b>3. Il Modello di organizzazione, gestione e controllo.....</b>	<b>14</b>
3.1 Adozione del Modello .....	14
3.2 Linee Guida di categoria.....	14
3.3 Definizione del Modello .....	16
3.4 Gli elementi base.....	17
3.5 La struttura del Modello .....	17
3.6 Piano di formazione e comunicazione.....	18
<b>4. L'Organismo di Vigilanza.....</b>	<b>20</b>
4.1 Identificazione dell'Organismo di Vigilanza .....	20
4.2 Caratteristiche dell'Organismo di Vigilanza.....	20
4.3 Composizione .....	20
4.4 Nomina, revoca e sostituzione .....	21
4.5 Funzionamento.....	22
4.6 Funzioni e poteri .....	23
4.7 Modalità di interazione con le altre funzioni aziendali .....	23
4.8 La gestione delle segnalazioni .....	24
4.9 Flusso di informazioni verso l'Organismo di Vigilanza .....	24
4.10 Reporting dell'Organismo di Vigilanza .....	24
4.11 I controlli dell'Organismo di Vigilanza.....	25
4.12 Raccolta e conservazione delle informazioni .....	26
<b>5. Il sistema disciplinare e sanzionatorio.....</b>	<b>27</b>
5.1 Disciplina sanzionatoria.....	27
5.2 Accertamento della violazione.....	27
5.3 Misure nei confronti dei dipendenti non dirigenti .....	27
5.4 Misure nei confronti dei dipendenti dirigenti.....	28
5.5 Misure nei confronti dei collaboratori esterni, intermediari e dei partner commerciali	28

5.6 Misure nei confronti del Rappresentante Generale o degli Amministratori .....	28
<b>Parte Speciale .....</b>	<b>29</b>
<b>1. Reati contro la Pubblica Amministrazione .....</b>	<b>29</b>
1.1 Analisi delle fattispecie di reato .....	29
1.2 Attività sensibili .....	31
1.3 Sistema dei controlli .....	33
<b>2. Reati societari .....</b>	<b>35</b>
2.1 Analisi delle fattispecie di reato .....	35
2.2 Attività sensibili .....	39
2.3 Sistema dei controlli .....	39
<b>3. Gestione delle risorse economiche e finanziarie .....</b>	<b>44</b>
3.1 Attività sensibili .....	44
3.2 Sistema dei controlli .....	44
<b>4. Abusi di mercato .....</b>	<b>47</b>
4.1 Analisi delle fattispecie di reato .....	47
4.2 Attività sensibili .....	50
4.3 Sistema dei controlli .....	50
<b>5. Reati con finalità di terrorismo o di eversione dell'ordine democratico .....</b>	<b>54</b>
5.1 Analisi delle fattispecie di reato .....	54
5.2. Attività sensibili .....	55
5.3 Sistema dei controlli interni.....	55
<b>6. Reati di ricettazione, riciclaggio e impiego di denaro, di beni o di utilità di provenienza illecita .....</b>	<b>58</b>
6.1 Analisi delle fattispecie di reato .....	58
6.2 Attività sensibili .....	59
6.3 Sistema dei controlli identificati in relazione alle attività sensibili individuate .....	59
<b>7. Delitti contro la personalità individuale .....</b>	<b>62</b>
7.1 Analisi delle fattispecie di reato .....	62
7.2 Attività sensibili .....	62
7.3 Sistema dei controlli .....	63
<b>8. Sicurezza sul lavoro .....</b>	<b>65</b>
8.1 Analisi delle fattispecie di reato .....	65
8.2 Attività sensibili .....	66
8.3 Sistema dei controlli .....	67
<b>9. Reati informatici e trattamento illecito di dati .....</b>	<b>70</b>
9.1 Analisi delle fattispecie di reato .....	70
9.2 Attività sensibili .....	73
9.3 Sistema dei controlli .....	74
<b>10. Altri reati .....</b>	<b>78</b>
10.1 Analisi delle fattispecie di reato .....	78
10.2 Attività sensibili .....	82
10.3 Sistema dei controlli .....	82
<b>Allegati.....</b>	<b>85</b>
<b>Attività sensibili- dettaglio per Società del Gruppo .....</b>	<b>85</b>

## Definizioni

- **“Attività Sensibili”**: attività esposte alla potenziale commissione dei reati contemplati dalla normativa e richiamati dal d. lgs. n. 231/2001.
- **“Casamadre”**: Helvetia Compagnia Svizzera di Assicurazioni SA;
- **“Codice Etico”**: Codice Etico del Gruppo Helvetia, Italia;
- **“Capogruppo” o “Rappresentanza”**: Compagnia Svizzera d'Assicurazioni SA Rappresentanza Generale e Direzione per l'Italia;
- **“Dipendenti”**: i soggetti aventi un rapporto di lavoro subordinato, ivi compresi i dirigenti, nonché i dipendenti in regime di somministrazione di lavoro che prestano la propria attività (cd. lavoratori interinali);
- **“Destinatari”**: sono, ai sensi dell'art. 5 del d. lgs. n. 231/2001, gli amministratori, i revisori contabili, i dirigenti, anche di fatto, i dipendenti, i collaboratori esterni (agenti, periti, consulenti, legali, fiduciari), gli intermediari ed i *partner* commerciali nei limiti dello svolgimento di attività nelle aree sensibili;
- **“D. Lgs n. 231/2001” o il “Decreto”**: il Decreto Legislativo dell'8 giugno 2001 n. 231 (*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*) e successive modifiche e integrazioni;
- **“Key Officer”**: persone di più alto livello organizzativo in grado di fornire le informazioni di dettaglio sui singoli processi aziendali e sulle attività delle singole funzioni.
- **“Modello di organizzazione, gestione e controllo” o “Modello”**: il modello di organizzazione, gestione e controllo predisposto ai sensi del d. lgs. n. 231/2001.
- **“Organismo di Vigilanza”**: organismo interno, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello nonché al relativo aggiornamento, ai sensi dell'art. 6 del d. lgs. n. 231/2001.
- **“Organo Amministrativo”**: Rappresentante Generale della Capogruppo e Consiglio di Amministrazione delle Società del Gruppo;
- **“Pubblica Amministrazione” o “Ente pubblico”**: enti pubblici territoriali e non territoriali (Stato, Regione, Provincia, Comune, Camera di Commercio, ASL, Ispettorato del Lavoro, etc.); enti istituiti e regolamentati con legge dello stato; società con partecipazione pubblica totalitaria o prevalente; società controllate da società con partecipazione pubblica totalitaria o prevalente; concessionario di pubblico servizio; la presenza di “poteri speciali” nello statuto delle società; società che debbono obbligatoriamente procedere alla stipulazione di contratti di fornitura di servizi attraverso il ricorso a gare d'appalto;
- **“Rappresentante Generale”**: Rappresentante Generale della Compagnia Svizzera d'Assicurazioni SA Rappresentanza Generale e Direzione per l'Italia;
- **“Società del Gruppo”**: Società del Gruppo Helvetia Italia composto da Compagnia Svizzera d'Assicurazioni SA Rappresentanza Generale e Direzione per l'Italia; Helvetia Vita SpA; Chiara Vita SpA; Padana Assicurazioni SpA; Ge.Si.Ass. S.c. a r.l.; APSA Srl;
- **“Soggetti Apicali” o “Apicali”**: persone che rivestono funzioni di rappresentanza, amministrazione o direzione o che esercitano, anche di fatto, la gestione e il controllo della stessa (art. 5, comma 1, d. lgs. n. 231/2001).

## Parte Generale

### 1. Decreto legislativo 8 giugno 2001 n. 231 e successive integrazioni e modificazioni

#### 1.1 La disciplina della responsabilità amministrativa

Il decreto legislativo 8 giugno 2001 n. 231 “Disciplina della responsabilità amministrativa delle persone giuridiche delle società e delle associazioni anche prive di personalità giuridica”, in attuazione della delega conferita al Governo con l’art. 11 della Legge 29 settembre 2000, n. 300<sup>1</sup>, disciplina la “*responsabilità degli enti per gli illeciti amministrativi dipendenti da reato*”, che si applica agli enti dotati di personalità giuridica e alle società e associazioni anche prive di personalità giuridica.

Il Decreto, in vigore dal 4 luglio 2001, ha introdotto la responsabilità amministrativa degli enti in aggiunta alla responsabilità penale della persona fisica che ha commesso il reato.

Secondo la disciplina introdotta dal Decreto, infatti, gli enti possono essere ritenuti responsabili per alcuni reati commessi o tentati, nell’interesse o a vantaggio degli stessi enti, da esponenti dei vertici aziendali, in posizione apicale, e da coloro che sono sottoposti alla direzione o vigilanza dei primi (art. 5, comma 1, del d. lgs. n. 231/2001)<sup>2</sup> e, quindi, sono soggetti, in via diretta ed autonoma, a determinate sanzioni amministrative in relazione ai reati ascritti ai citati soggetti.

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

#### 1.2 I reati presupposto

In base al Decreto, la società può essere ritenuta responsabile soltanto per i reati espressamente richiamati da specifiche disposizioni normative. Nel corso degli anni si è assistito ad un progressivo “allargamento” degli illeciti con riferimento ai quali si applica la normativa in esame.

Le fattispecie richiamate dal d. lgs. n. 231/2001 possono essere comprese, per comodità espositiva, nelle seguenti categorie:

- **delitti contro la Pubblica Amministrazione.** Si tratta del primo gruppo di reati originariamente individuato dagli articoli 24 e 25 del Decreto e, in particolare, di: malversazione a danno dello Stato o dell’Unione Europea (art. 316-*bis* c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.), truffa in danno dello Stato o di altro ente pubblico (art. 640 comma 2, n. 1 c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.), frode informatica in danno dello Stato e di altro ente pubblico (art. 640-*ter* c.p.), concussione (art. 317 c.p.), corruzione per un atto d’ufficio e corruzione per un atto contrario ai doveri d’ufficio (artt. 318, 319 e 319-*bis* c.p.), corruzione in

---

<sup>1</sup> La legge 29 settembre 2000, n. 300, nel delegare al governo la definizione di un sistema di responsabilità sanzionatoria amministrativa degli enti e delle società, ha ottemperato agli obblighi previsti da alcuni protocolli e convenzioni internazionali ratificate dall’Italia, relative alla responsabilità degli enti collettivi per talune fattispecie di reato, tra le quali la Convenzione sulla tutela degli interessi finanziari delle Comunità europee (Bruxelles, 26 luglio 1995) e relativo primo Protocollo (Dublino, 27 settembre 1996), la Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell’Unione europea (Bruxelles, 26 maggio 1997), la Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali (Parigi, 17 dicembre 1997).

<sup>2</sup> Art. 5, comma 1, del d.lgs. n. 231/2001: “Responsabilità della società – *La società è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)*”.

atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), delitti del corruttore (art. 321 c.p.), istigazione alla corruzione (art. 322 c.p.), concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e degli Stati esteri (art. 322-bis c.p.);

- **delitti contro la fede pubblica**, previsti dall'art. 25-bis del Decreto e introdotti dalla legge 23 novembre 2001 n. 409 (art. 6), recante "Disposizioni urgenti in vista dell'introduzione dell'Euro". Si tratta dei reati di falsità in monete, in carte di pubblico credito e in valori di bollo;
- **reati societari**, richiamati dall'art. 25-ter d. lgs. n. 231/2001. Il D. Lgs. 11 aprile 2002, n. 61, nell'ambito della riforma del diritto societario, ha previsto l'estensione del regime di responsabilità amministrativa degli enti anche ai reati di false comunicazioni sociali (art. 2621 c.c., così come modificato dall'art. 30, primo comma, della legge n. 262/2005), false comunicazioni sociali in danno della società, dei soci e dei creditori (art. 2622 c.c., così come modificato dall'art. 30, secondo comma, della legge n. 262/2005), falso in prospetto (art. 173-bis TUF), falsità nelle relazioni o nelle 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.), omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.), formazione fittizia del capitale (art. 2632 c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), illecita influenza dell'assemblea (art. 2636), agiotaggio (art. 2637 c.c.), ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638 c.c.);
- **delitti in materia di terrorismo e di eversione dell'ordine democratico** (richiamati dall'art. 25-quater d. lgs. n. 231/2001, introdotto dall'art. 3 della legge 14 gennaio 2003, n. 7). Si tratta dei "delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali", nonché dei delitti, diversi da quelli sopra indicati, "che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999");
- **abusi di mercato** (indicati dall'art. 25-sexies Decreto, introdotto dall'art. 9 della legge 18 aprile 2005, n. 62 ("Legge Comunitaria 2004"). La norma prevede che la società possa essere chiamata a rispondere dei reati di abuso di informazioni privilegiate (art. 184 TUF) e manipolazione del mercato (art. 185 TUF). In base all'art. 187-quinquies del TUF, la società può essere, altresì, ritenuto responsabile del pagamento di una somma pari all'importo della sanzione amministrativa pecuniaria irrogata per gli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-bis TUF) e di manipolazione del mercato (187-ter TUF), se commessi, nel suo interesse o a suo vantaggio, da persone riconducibili alle categorie dei "soggetti apicali" e dei "soggetti sottoposti all'altrui direzione o vigilanza";
- **delitti contro la personalità individuale** (previsti dall'art. 25-quinquies del Decreto, introdotto dall'art. 5 della legge 11 agosto 2003, n. 228). I reati sanzionati consistono nella riduzione o mantenimento in schiavitù o in servitù, la prostituzione minorile, la pornografia minorile, la detenzione di materiale pornografico, la pornografia virtuale, le iniziative turistiche volte allo sfruttamento della prostituzione minorile;
- **reati transnazionali**. L'art. 10 della legge 16 marzo 2006 n. 146 prevede la responsabilità amministrativa della società anche con riferimento ai reati transnazionali individuati dalla stessa legge: associazione per delinquere (art. 416 c.p.), associazione per delinquere di tipo mafioso (art. 416-bis c.p.), associazione finalizzata al contrabbando di tabacchi lavorati esteri (D.P.R. n. 43/1973, 291-quater), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (D.P.R. n. 309/1990, art. 74), traffico di migranti (d. lgs. 286/1998, art. 12, comma 3, 3-bis, 3-ter, 5) ed alcuni reati di intralcio alla giustizia, quali l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) e il favoreggiamento personale (art. 378 c.p.). L'illecito è considerato transnazionale

quando sia stato commesso in più di uno Stato, ovvero, se commesso in uno Stato, una parte sostanziale della preparazione e pianificazione dell'illecito sia avvenuta in altro Stato, ovvero ancora se commesso in uno Stato, in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più Stati;

- **delitti contro la vita e l'incolumità individuale.** L'art. 25-*quater*.1 del Decreto prevede tra i delitti con riferimento ai quali è riconducibile la responsabilità amministrativa della società le pratiche di mutilazione degli organi genitali femminili;
- **omicidio colposo e lesioni colpose gravi e gravissime commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.** L'art. 25-*septies*<sup>3</sup> prevede la responsabilità amministrativa in relazione ai delitti di cui agli articoli 589 e 590, terzo comma, del codice penale (Omicidio colposo e lesioni colpose gravi o gravissime), commessi con violazione delle norme poste a tutela della salute e della sicurezza sul lavoro;
- **reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.** L'art. 25-*octies*<sup>4</sup> del Decreto ha esteso la responsabilità della società anche con riferimento ai reati previsti dagli artt. 648, 648-*bis* e 648-*ter* del codice penale;
- **delitti informatici e trattamento illecito di dati.** L'art. 24-*bis* del Decreto prevede fattispecie di illecito amministrativo in dipendenza di taluni delitti informatici e trattamento illecito di dati<sup>5</sup>;
- **delitti di criminalità organizzata.** L'art. 24-*ter* del Decreto prevede fattispecie di reato contro in materia di sicurezza pubblica<sup>6</sup>;
- **delitti contro l'industria e il commercio.** L'art. 25-*bis*-1 del Decreto prevede fattispecie di reato in materia di fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale<sup>7</sup>;
- **delitti in materia di violazioni del diritto d'autore.** L'art. 25-*nonies* del Decreto prevede fattispecie di reato in materia di abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere televisive, cinematografiche, musicali, letterarie, scientifiche o didattiche tutelate dal diritto di autore<sup>8</sup>;

3 Il citato articolo è stato introdotto dall'art. 9, legge 3 agosto 2007, n. 123 e successivamente, modificato dall'art. 300 (Modifiche al decreto legislativo 8 giugno 2001, n. 231) del d.lgs. 9 aprile 2008 n. 81 recante attuazione dell'art. 1 della legge 3 agosto 2007 n. 123 in materia di tutela della salute e sicurezza sui luoghi di lavoro.

4 L'art. 63, comma 3, del d.lgs. 21 novembre 2007, n. 231, pubblicato sulla Gazzetta Ufficiale 14 dicembre 2007 n. 290, S.O. n. 268, recante attuazione della direttiva 2005/60/CE del 26 ottobre 2005 e concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva n. 2006/70/CE, che ne reca le misure di esecuzione, ha introdotto il nuovo articolo nel decreto legislativo 8 giugno 2001, n. 231, il quale prevede, appunto, la responsabilità amministrativa della società anche nel caso di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

5 L'art. 24-*bis* è stato introdotto nel testo del d.lgs. n. 231/2001 dall'art. 7 della legge 18 marzo 2008 n. 48 recante ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno, pubblicata sulla G.U. n. 80 del 4 aprile 2008 – S.O. n. 79. I delitti dai quali deriva la responsabilità amministrativa degli enti sono quelli di cui agli artt. 491-*bis* (Falsità in documenti informatici), 615-*ter* (Accesso abusivo ad un sistema informatico o telematico), 615-*quater* (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici), 615-*quinquies* (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico), 617-*quater* (Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche), 617-*quinquies* (Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche), 635-*bis* (Danneggiamento di informazioni, dati e programmi informatici), 635-*ter* (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), 635-*quater* (Danneggiamento di sistemi informatici o telematici), 635-*quinquies* (Danneggiamento di sistemi informatici o telematici di pubblica utilità) e 640-*quinquies* (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica) del codice penale. Sul tema dei c.d. crimini informatici: Ruggieri, Cyber crime e responsabilità amministrativa degli enti, Diritto e pratica delle società, n. 8/2008, Milano, pag. 6 e ss.

6 Articolo aggiunto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29 (G.U. n. 170 del 24 luglio 2009).

7 Articolo aggiunto dalla Legge 23 Luglio 2009, n.99, art.15 (G.U. N. 176 del 31 luglio 2009).

8 Articolo aggiunto dalla Legge 23 luglio 2009 n. 99, art. 15 (G.U. N. 176 del 31 luglio 2009).

- **induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.** L'art. 25-novies del Decreto prevede fattispecie di reato in materia di dichiarazioni mendaci all'autorità giudiziaria<sup>9</sup>.

### 1.3 Elementi chiave del Decreto

Il concetto innovativo introdotto dal Decreto nell'ordinamento giuridico italiano è rappresentato dall'introduzione di un nuovo tipo di responsabilità a carico degli enti. Ad essi sono ora applicabili sanzioni, in via diretta ed autonoma, in relazione a illeciti, commessi nel loro interesse o nel loro vantaggio, da soggetti ad essi funzionalmente legati ai sensi dell'art. 5 del Decreto.

La responsabilità degli enti e delle società è indipendente da quella delle persone fisiche che hanno realizzato materialmente il fatto nell'interesse o a vantaggio della società stessa.

Infatti essa sussiste anche quando l'autore del reato non sia stato identificato, o non sia imputabile, e quando il reato si estingue per una causa diversa dall'amnistia.

La responsabilità amministrativa della società è, tuttavia, esclusa se la società ha, tra l'altro, adottato ed efficacemente attuato, prima della commissione dei reati, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi; tali modelli possono essere adottati sulla base di linee guida e codici di comportamento elaborati dalle associazioni di categoria.

### 1.4 Autori del reato

La società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da *“persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo della società”*, ovvero dai soggetti in posizione apicale (art. 5, comma 1, lett. a), del d. lgs. n. 231/2001);
- da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (*“soggetti sottoposti all'altrui direzione o vigilanza”* (art. 5, comma 1, lett. b, del d. lgs. n. 231/2001).

È opportuno, altresì, ribadire che la società non risponde, per espressa previsione legislativa (art. 5, comma 2, del d. lgs. n. 231/2001), se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi<sup>10</sup>.

### 1.5 Natura della responsabilità

Con riferimento alla natura della responsabilità amministrativa ex d. lgs. n. 231/2001, la Relazione illustrativa al decreto sottolinea la *“nascita di un tertium genus che coniuga i tratti essenziali del sistema penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle, ancor più ineludibili, della massima garanzia”*.

Il d. lgs. n. 231/2001 ha, infatti, introdotto nel nostro ordinamento una forma di responsabilità delle società di tipo amministrativo, in ossequio al dettato dell'art. 27 della nostra Costituzione<sup>11</sup>, ma con numerosi punti di contatto con una responsabilità di tipo penale.

<sup>9</sup> Articolo aggiunto dalla L. 3 agosto 2009 n. 116, art. 4 (G.U. N. 188 del 14 agosto 2009).

<sup>10</sup> Art. 5, comma 2, del d.lgs. n. 231/2001: *“Responsabilità della società – La società non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi”*.

<sup>11</sup> Art. 27 comma 1 della Costituzione della Repubblica Italiana: *“La responsabilità penale è personale”*.

## 1.6 Le sanzioni previste

Il d. lgs. n. 231/2001 prevede a carico della società, in conseguenza della commissione o tentata commissione dei reati sopra menzionati, una serie articolata di sanzioni, classificabili in quattro tipologie:

- 1) **sanzioni pecuniarie** (artt. 10 - 12 d. lgs. n. 231/2001). Le sanzioni pecuniarie si applicano sempre, anche nel caso in cui la società ripari alle conseguenze del reato stesso. La sanzione pecuniaria ha natura esclusivamente afflittiva e non risarcitoria, dunque è diretta a punire la società e non a risarcire il danno.

La sanzione pecuniaria è determinata dal giudice penale attraverso un sistema basato su "quote" in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 ad un massimo di Euro 1.549,37. Nella commisurazione della sanzione pecuniaria il giudice determina:

- il numero delle quote, tenendo conto della gravità del fatto, del grado della responsabilità della società nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- l'importo della singola quota, sulla base delle condizioni economiche e patrimoniali della società.

- 2) **sanzioni interdittive** (artt. 13 - 17 d. lgs. n. 231/2001). Tali sanzioni, il cui effetto è quello di paralizzare o ridurre l'attività della società<sup>12</sup>, di durata non inferiore a tre mesi e non superiore a due anni a loro volta, possono consistere in:

- interdizione all'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, ed eventuale revoca di quelli già concessi;
- divieto di pubblicizzare beni o servizi.

In luogo dell'irrogazione della sanzione interdittiva, il giudice può disporre la prosecuzione dell'attività della società da parte di un commissario nominato dal giudice (ai sensi e alle condizioni di cui all'art. 15 del d. lgs. n. 231/2001).

Le sanzioni interdittive possono applicarsi solo in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni:

- la società ha tratto dal reato un profitto di "rilevante" entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- sono stati commessi altri precedenti illeciti ai sensi del d. lgs. n. 231/2001 dello stesso tipo di quelli accertati dal giudice.

- 3) **Pubblicazione della sentenza** (art. 18 d. lgs. n. 231/2001).

- 4) **Confisca** (art. 19 d. lgs. n. 231/2001): si tratta della confisca del profitto che la società ha tratto dal reato.

---

<sup>12</sup> Si precisa che, ai sensi dell'art. 14, comma 1, d.lgs. n. 231/2001, "Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito della società".

### **1.7 La responsabilità della società**

Il Decreto ha diversificato il sistema di responsabilità della società a seconda che il reato sia stato commesso da un soggetto in posizione apicale o da un soggetto sottoposto alla direzione o alla vigilanza di un soggetto in posizione apicale.

### **1.8 Soggetti in posizione apicale**

Quando il reato è stato commesso da soggetti in posizione apicale, la responsabilità della società è presunta. La stessa società dovrà, dunque, dimostrare la sua estraneità ai fatti contestati al soggetto apicale provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di riflesso, la circostanza che la commissione del reato non deriva da una propria "*colpa organizzativa*" provando la sussistenza dei seguenti requisiti (art. 6, comma 1, d. lgs. n. 231/2001):

- l'adozione da parte dell'organo dirigente e l'efficace attuazione, prima della commissione del fatto, di un Modello di organizzazione, di gestione e di controllo idoneo a prevenire reati previsti dal Decreto;
- l'affidamento a un Organismo di Vigilanza della società dotato di autonomi poteri di iniziativa e di controllo di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento;
- l'elusione fraudolenta del Modello da parte delle persone che hanno commesso il reato;
- l'assenza di omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, il Modello deve:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

### **1.9 Soggetti sottoposti a direzione o vigilanza del soggetto apicale**

Quando il reato è stato commesso da soggetto sottoposto a direzione o vigilanza del soggetto apicale, l'onere probatorio è, a differenza di quanto previsto per i soggetti in posizione apicale, a carico dell'Autorità Giudiziaria.

La società è ritenuta responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. L'inosservanza di tali obblighi è, comunque, esclusa se la stessa società, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi che preveda, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

L'art. 7, comma 4, del d. lgs. n. 231/2001 definisce, inoltre, i requisiti dell'efficace attuazione dei modelli organizzativi:

- una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

## **2. Attività e organizzazione**

### **2.1 Aspetti organizzativi**

Helvetia Group è un gruppo europeo fornitore di servizi assicurativi presente nel mercato italiano attraverso il Gruppo Assicurativo Helvetia Italia, che attualmente è formato dalle seguenti società:

- Helvetia Compagnia Svizzera d'Assicurazioni SA – Rappresentanza Generale e Direzione per l'Italia in qualità di Capogruppo;
- Helvetia Vita S.p.A., detenuta al 100% da Helvetia Europe SA;
- Padana Assicurazioni S.p.A., detenuta al 100% dalla Rappresentanza Generale per l'Italia;
- Chiara Vita S.p.A., detenuta al 70% da Helvetia Europe SA;
- Ge.Si.Ass. S.c. a r.l., detenuta al 40% dalla Rappresentanza Generale per l'Italia e per il 5% ciascuno da Helvetia Vita S.p.A., Padana Assicurazioni S.p.A. e Chiara Vita S.p.A.;
- APSA Srl detenuta al 60% da Padana Assicurazioni S.p.A.

I prodotti assicurativi sono collocati tramite diverse tipologie di intermediari (agenti, broker, sportelli bancari, ecc.)

#### **Helvetia Assicurazioni SA, Italia**

Helvetia Assicurazioni SA, Italia è la Rappresentanza Generale e Direzione per l'Italia della Helvetia Compagnia Svizzera d'Assicurazioni SA ed ha per oggetto l'esercizio di assicurazione e riassicurazione privata nei Rami Danni.

#### **Helvetia Vita S.p.A.**

Helvetia Vita S.p.A - Compagnia di Assicurazioni è una società di diritto italiano che ha per oggetto l'esercizio di ogni specie di assicurazione e riassicurazione privata sulla Vita, di capitalizzazione e può procedere alla costituzione ed alla gestione di Fondi Pensione Aperti.

#### **Chiara Vita S.p.A.**

Chiara Vita S.P.A. - Compagnia di Assicurazioni ha per oggetto l'esercizio in Italia e all'estero delle assicurazioni nei rami vita in tutte le forme, ivi comprese le assicurazioni complementari per danni alla persona, le operazioni di capitalizzazione e la riassicurazione negli stessi rami. Inoltre, la società può costituire fondi pensione aperti.

#### **Padana Assicurazioni S.p.A.**

Padana Assicurazioni SpA ha per oggetto l'esercizio delle assicurazioni e delle riassicurazioni in tutti i rami e nelle loro varie forme e combinazioni, principalmente nel comparto dei rischi "Auto e Persone". La Società può svolgere la sua attività sia in Italia sia all'estero.

#### **Ge.Si.Ass. S.c. a r.l.**

Ge.Si.Ass. Gestione Sistemi Assicurativi - Società Consortile a Responsabilità Limitata ha per oggetto la gestione di sistemi informativi, lo sviluppo e la gestione di software applicativi e l'elaborazione di dati, il tutto per conto delle imprese socie.

### **APSA S.r.l.**

APSA Srl ha per oggetto l'attività di intermediazione assicurativa in tutti i rami effettuata mediante l'assunzione e la gestione di mandati di agenzia da parte di compagnie assicurative. La società, attualmente mandataria di Padana Assicurazioni S.p.A. e Helvetia Vita S.p.A., può acquisire mandati assicurativi e svolgere attività di promozione, conclusione, raccolta, gestione ed organizzazione di prodotti assicurativi e/o complementari nei limiti dei mandati assunti.

## **2.2 Governance e sistema di controllo interno**

La Governance della Casamadre tramite la Capogruppo e le Società del Gruppo costituisce uno degli aspetti fondamentali per garantire l'efficacia del Modello, in quanto inerente agli aspetti relativi alla ripartizione dei poteri e delle responsabilità.

Il Rappresentante Generale ha un ruolo di coordinamento di tutte le Società del Gruppo operanti in Italia, di presidio della Corporate Governance e compliance e riporta al Board of Directors di Casamadre.

La struttura delle Società del Gruppo viene comunicata attraverso l'organigramma in vigore, reso disponibile nell'intranet aziendale da parte dell'Unità Risorse Umane e Servizi.

Le più importanti modifiche strutturali sono rese note ai dipendenti del Gruppo attraverso specifiche comunicazioni.

Semestralmente viene inviato ai Dirigenti del Gruppo l'organigramma dettagliato.

Coerentemente con il Regolamento n. 20 del 26 marzo 2008, le Società del Gruppo hanno istituito:

- la funzione di Internal Audit, incaricata di monitorare e valutare l'efficacia e l'efficienza del sistema di controllo interno e le necessità di adeguamento, anche attraverso attività di supporto e di consulenza alle altre funzioni aziendali;
- la funzione di Risk Management per la gestione dei rischi attraverso l'identificazione, la valutazione e il controllo dei rischi;
- la funzione di Compliance incaricata di prevenire il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di leggi, regolamenti o provvedimenti delle Autorità di Vigilanza ovvero di norme di autoregolamentazione.

La società di revisione esterna incaricata svolge le proprie attività di controllo contabile secondo i principi di revisione consolidati ed attuando le opportune sinergie con la struttura di Internal Audit.

## **2.3 Valori di riferimento e normativa interna**

I valori di riferimento sono diffusi attraverso Codice Etico e *Policy* specifiche che indirizzano i comportamenti di dipendenti e di collaboratori nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive di Gruppo.

Tali documenti sono consegnati o resi disponibili a ciascun dipendente che è tenuto a conoscerli ed applicarne i contenuti, ove ad esso rilevanti.

### 3. Il Modello di organizzazione, gestione e controllo

#### 3.1 Adozione del Modello

La decisione di adottare un Modello, da parte della Capogruppo per tutte le Società del Gruppo, oltre a rappresentare un sistema di prevenzione dalla commissione di alcune tipologie di reato, è un atto di responsabilità sociale che rientra nel quadro di un impegno più generale, assunto sia nei confronti dei propri azionisti, clienti, dipendenti, fornitori e concorrenti, sia nei confronti di quanti siano interessati all'attività delle stesse.

Il Rappresentante Generale della Capogruppo informa dell'adozione del Modello il Board of Directors di Casamadre seguendo i processi interni.

L'introduzione del Modello ha permesso, infatti, di consolidare e rafforzare:

- la cultura dell'integrità aziendale, riducendo i rischi legali connessi a comportamenti non etici e favorendo la sensibilizzazione dei dipendenti;
- la credibilità verso gli stakeholder (clienti, fornitori, collaboratori, ambiente, azionisti e società civile) e le istituzioni pubbliche, potenziando la reputazione aziendale;
- la diffusione dell'eticità del business, promuovendo la cultura del controllo;
- la trasparenza nella comunicazione interna ed esterna, riducendo la conflittualità sociale e favorendo l'allineamento dei comportamenti individuali alle strategie ed agli obiettivi aziendali.

L'adozione del Modello rappresenta, dunque, uno strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto delle Società del Gruppo, a svolgere le proprie attività con comportamenti corretti e lineari, al fine di prevenire e ridurre il rischio di commissione dei reati contemplati dal Decreto.

#### 3.2 Linee Guida di categoria

L'art. 6, comma 3, del d. lgs. n. 231/2001 prevede che *"I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati"*.

Tale previsione normativa ha principalmente la finalità di promuovere, nell'ambito degli aderenti alle associazioni di categoria, l'allineamento ai principi espressi dal Decreto e, parimenti, di stimolare l'elaborazione di codici strutturati che possano fungere da punto di riferimento per gli operatori che si accingano a redigere un modello di organizzazione e gestione.

L'Associazione Nazionale per le Imprese Assicuratrici (ANIA) ha emanato le "Linee Guida per il Settore Assicurativo in materia di responsabilità amministrativa" elaborate per il settore assicurativo, ai sensi dell'art. 6, comma 3, del decreto legislativo 8 giugno 2001, n. 231, al fine di predisporre una base per l'eventuale adozione da parte delle singole imprese assicuratrici di un "modello di organizzazione e gestione" idoneo, ai sensi dello stesso art. 6, comma 1, lett. a), a prevenire i reati e gli illeciti considerati dal decreto predetto.

Le Linee Guida sono coerenti con le disposizioni in materia di controllo interno per le imprese di assicurazione e in particolare con il Regolamento n. 20 del 26 marzo 2008 *"Regolamento recante disposizioni in materia di controlli interni, gestione dei rischi, Compliance ed esternalizzazione delle attività delle imprese di assicurazione, ai sensi degli articoli 87 e 191, comma 1, del decreto legislativo 7 settembre 2005, n. 209 – Codice delle assicurazioni private"*.

Tale normativa evidenzia l'importanza di un sistema articolato di attenzione e vigilanza nell'ambito aziendale che comprenda sia un controllo diretto a garantire la solvibilità dell'impresa di assicurazione e la sua sana e prudente gestione, e quindi anche la soddisfazione degli obiettivi strategici delineati dal vertice aziendale e l'attuazione delle istruzioni impartite dallo stesso vertice a tutela della stabilità dell'impresa e contro i pericoli che possono derivare da violazioni della disciplina pubblicistica del settore assicurativo o della legge in genere, nel quadro di uno sviluppo equilibrato dell'impresa e di una complessiva vigilanza prudenziale tipica dei settori finanziari, sia un controllo diretto alla assunzione di misure tali da impedire a tutti, compreso lo stesso vertice dell'impresa, di commettere o far commettere reati e illeciti nell'interesse o a vantaggio dell'impresa medesima.

Ne risulta un generale e complesso "sistema di controlli interni" che richiede continue attività e coinvolge gli organi di vertice, le strutture aziendali e il personale tutto, divenendo elemento integrante dell'azienda, che prevede:

- i controlli di linea, diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture produttive (ad es., i controlli di tipo gerarchico) o incorporati nelle procedure ovvero eseguiti nell'ambito dell'attività di back-office;
- i controlli sulla gestione dei rischi, che hanno l'obiettivo di concorrere alla definizione delle metodologie di misurazione del rischio, di verificare il rispetto dei limiti assegnati alle varie funzioni operative e di controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio/rendimento assegnati. Essi sono affidati a strutture diverse da quelle produttive;
- i controlli sulla gestione del rischio di conformità, che hanno l'obiettivo di identificare in via continuativa le norme applicabili all'impresa e valuta il loro impatto sui processi e le procedure aziendali, valutare l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e propone le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio, di valutare l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite e di predisporre adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.
- l'attività di revisione interna, volta a individuare andamenti anomali, violazioni delle procedure e della regolamentazione nonché a valutare la funzionalità del complessivo sistema dei controlli interni. Essa è condotta nel continuo, in via periodica o per eccezioni, da strutture diverse e indipendenti da quelle produttive, anche attraverso verifiche in loco.

Il sistema dei controlli interni consente di dotarsi di standard organizzativi ottimali, in linea con il principio di sana gestione, il quale costituisce, seppure in una accezione più ampia, ciò che il Decreto intende affermare nell'ordinamento. Sono pertanto operative un insieme di regole, di procedure e di strutture organizzative che devono mirare ad assicurare il rispetto delle strategie aziendali ed il conseguimento della efficacia e dell'efficienza dei processi aziendali; la salvaguardia del valore delle attività e la protezione dalle perdite; l'affidabilità e l'integrità delle informazioni contabili e gestionali; la conformità delle operazioni con la legge, con la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne.

Alla luce di tale sistema normativo, le associazioni di categoria elencano e descrivono gli elementi fondamentali e le componenti di un modello di organizzazione idoneo a prevenire i reati di cui al Decreto. In particolare il modello organizzativo deve prevedere:

- l'individuazione delle attività nel cui ambito possono essere commessi i reati;
- la previsione di regole dirette a programmare la formazione e l'attuazione delle decisioni in relazione ai reati da prevenire e individuazione delle modalità di gestione delle risorse finanziarie: Codice Etico e Policy;

- la nomina di un organismo di controllo interno che abbia il compito di vigilare sul funzionamento e l'osservanza del modello organizzativo e gestionale adottato dalla società, e di curarne l'aggiornamento;
- la previsione di obblighi di informazione nei confronti dell'organismo deputato al controllo;
- la presenza di sistema di verifica periodica e di eventuale aggiornamento del modello organizzativo;
- la definizione di un idoneo sistema disciplinare e sanzionatorio con riferimento al rispetto del modello organizzativo stesso e delle norme di comportamento previste;
- la diffusione del modello organizzativo adottato;
- la formazione del personale in materia di responsabilità amministrativa degli enti e sulle componenti del modello adottato.

### 3.3 Definizione del Modello

Il Modello prevede come requisiti l'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati espressamente richiamati dal Decreto. Si tratta, in altri termini, di quelle attività e processi aziendali che comunemente vengono definite "attività sensibili".

L'individuazione delle attività sensibili prevede l'analisi, documentale seguita da interviste dirette al personale, relativamente alla struttura societaria ed organizzativa, svolta al fine di meglio comprendere l'attività della stessa e di identificare gli ambiti aziendali oggetto dell'intervento.

La raccolta della documentazione rilevante e l'analisi della stessa da un punto di vista sia tecnico-organizzativo, sia legale permette l'individuazione delle attività sensibili e una preliminare identificazione delle funzioni responsabili delle attività sensibili, ovvero quelle risorse con una conoscenza approfondita di tali processi operativi e dei meccanismi di controllo in essere in grado di fornire il supporto necessario a dettagliare le attività sensibili ed i relativi meccanismi di controllo.

In particolare, i *Key Officer* sono identificati nelle persone di più alto livello organizzativo in grado di fornire le informazioni di dettaglio sui singoli processi aziendali e sulle attività delle singole funzioni.

L'individuazione delle attività sensibili, coinvolge l'intero perimetro aziendale ed è condotta tramite interviste dirette che hanno interessato i Key Officer identificati. Tali interviste hanno avuto anche lo scopo di stabilire, per ogni attività sensibile individuata, i processi di gestione e gli strumenti di controllo, con particolare attenzione agli elementi di compliance e ai controlli preventivi esistenti.

Nella rilevazione del sistema di controllo esistente si sono presi, tra l'altro, come riferimento, i seguenti principi di controllo:

- segregazione dei compiti;
- esistenza di normativa aziendale formalizzata ed approvata dagli organi muniti dei necessari poteri;
- esistenza di deleghe formalizzate coerenti con le responsabilità organizzative assegnate;
- tracciabilità e verificabilità ex post delle operazioni tramite adeguati supporti documentali e informativi.

Il processo di identificazione delle attività sensibili ha previsto la predisposizione di un documento nel quale sono state descritti i controlli previsti e le funzioni coinvolte nei processi, ai sensi del Decreto.

### 3.4 Gli elementi base

Il Modello di organizzazione adottato si fonda su un insieme integrato di metodologie e strumenti, composto principalmente dai seguenti elementi:

- Codice Etico, che è portata a conoscenza anche dei soggetti esterni sui quali la società esercita un potere di direzione o di vigilanza e di coloro che intrattengono rapporti stabili di affari con la società stessa, nonché, più in generale, di quanti siano portatori di interessi nei suoi confronti;
- organigramma, complessivo e dettagliato, per una chiara individuazione della struttura gerarchica e funzionale;
- principi e logiche di attribuzione delle deleghe di poteri per governare il conferimento delle facoltà di compiere atti attinenti l'esercizio;
- procedure interne per la regolamentazione delle attività operative, la definizione dei livelli di controllo e degli iter autorizzativi;
- sistema informativo, costituito dall'insieme degli strumenti hardware e software atto a supportare la gestione dei dati e le informazioni utilizzate nello svolgimento delle attività;
- meccanismo di rilevazione segnalazioni, per assicurare che chiunque ravvisi situazioni di possibile violazione delle norme prescritte possa informare le strutture competenti senza pericoli di ritorsione;
- sistema disciplinare interno che definisce il procedimento e i provvedimenti disciplinari volti a sanzionare il mancato rispetto delle misure indicate nel Modello e nelle procedure ad esso correlate;
- programma di sensibilizzazione, formazione e informazione sui contenuti del Modello;
- flussi di comunicazione da e verso l'Organismo di Vigilanza;
- documentazione e verbalizzazione delle attività di verifica, di controllo e di intervento svolte dall'Organismo di Vigilanza.

### 3.5 La struttura del Modello

Il Modello è costituito da una Parte Generale e da una Parte Speciale.

La Parte Generale contiene le regole e le considerazioni di carattere generale del Modello che descrive, oltre che l'insieme delle informazioni generali riguardanti il profilo organizzativo e i principi etici e di Corporate Governance, anche il processo di definizione ed i principi di funzionamento del Modello, nonché i meccanismi di concreta attuazione dello stesso.

La Parte Speciale contiene le diverse categorie di reato contemplate nel Decreto, l'identificazione delle attività sensibili e dei presidi di controllo da adottare a fini preventivi, per le quali sono collegate delle specifiche schede di analisi in merito ai controlli in essere ed alle unità organizzative coinvolte.

In particolare sono stati individuati i seguenti reati potenziali:

- "Reati commessi nei rapporti con la Pubblica Amministrazione", trova applicazione per le tipologie specifiche di reati individuati dagli artt. 24 e 25 del Decreto.
- "Reati Societari", si applica per le tipologie specifiche di reati individuati dall'art. 25-ter del Decreto.

- “Gestione delle risorse economiche e finanziarie” fa riferimento ai processi di gestione delle risorse da parte dei soggetti in posizione apicale, per i quali sono state individuati norme e principi di comportamento, unitamente ai controlli diretti a verificarne il rispetto e l’attuazione.
- “Abusi di mercato”, si applica per le tipologie specifiche di reati specificati dall’art. 25-sexies del Decreto e di illeciti amministrativi specificati dall’art. 187-quinquies TUF.
- “Reati con finalità di terrorismo o di eversione dell’ordine democratico”, si applica per le tipologie di reati specificati dall’art. 25-quater del Decreto.
- “Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita” si riferisce ai delitti individuati dall’art. 25-octies del Decreto. Tali delitti, che prima dell’introduzione di tale articolo, erano sanzionati ai sensi del Decreto soltanto quando assumevano la caratteristica della “trans nazionalità”, ora sono divenuti sanzionabili indipendentemente da tale caratteristica, sempre che ne derivi un interesse o vantaggio per la società.
- “Delitti contro la personalità individuale”, si applica per le tipologie di delitti previsti dall’art. 25-quinquies del Decreto.
- “Sicurezza sul lavoro” è relativa alle regole di comportamento ed ai presidi di controllo che garantiscono il rispetto della normativa antinfortunistica e di tutela dell’igiene e della salute sul lavoro.
- “Delitti informatici e trattamento illecito dei dati” è relativa alle regole di comportamento ed ai presidi di controllo con riferimento ai delitti informatici e trattamento illecito dei dati di cui all’art. 24- bis del Decreto;
- “Delitti di criminalità organizzata” relativi ai reati contro in materia di sicurezza pubblica di cui all’art. 24-ter del Decreto;
- “Delitti contro l’industria e il commercio” relativi ai reati in materia di fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale, di cui all’art. 25-bis-1 del Decreto;
- “Delitti in materia di violazioni del diritto d’autore” relativi ai reati in materia di di abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere televisive, cinematografiche, musicali, letterarie, scientifiche o didattiche tutelate dal diritto di autore, di cui all’art. 25-nonies del Decreto;
- “Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria” relativi ai reati in materia di dichiarazioni mendaci all’Autorità Giudiziaria, di cui all’art. 25-novies del Decreto.

### 3.6 Piano di formazione e comunicazione

Al fine di dare efficace attuazione al Modello adottato, il Modello è comunicato ai dipendenti e a quanti, pur non rivestendo la qualifica formale di dipendenti, operano per il conseguimento degli obiettivi, svolgendo attività nelle aree definite come sensibili. L’attività di informazione concernente i contenuti ed i principi del Modello, diversamente caratterizzata a seconda dei destinatari cui essa si rivolge, è improntata a completezza, tempestività, accuratezza e continuità al fine di consentire la piena consapevolezza delle disposizioni aziendali che sono tenuti a rispettare.

Gli strumenti adottati per effettuare una comunicazione efficace sono i seguenti:

- i contenuti ed i principi del Modello che essi sono tenuti a conoscere sono portati a conoscenza dei Dipendenti sia con la consultazione del documento direttamente sull’*intranet* aziendale e sia tramite percorsi formativi, in relazione al ruolo ed alle responsabilità rivestite;

- copia del Modello è disponibile sul sito internet della Società ed è destinata ai soggetti che intrattengono rapporti di collaborazione contrattualmente regolati e coinvolti nello svolgimento di attività sensibili, con particolare attenzione a quanti sono soggetti alla direzione o alla vigilanza. In questo caso i contratti e le lettere di incarico prevedono clausole di “*non violazione del Modello di organizzazione, gestione e controllo*”, anche per incarichi trasferiti a terze parti domiciliatarie;
- è data facoltà ai Dipendenti di contattare l'Organismo di Vigilanza per eventuali chiarimenti sui comportamenti da adottare al fine di rispettare i principi enunciati nel Modello adottato.

## **4. L'Organismo di Vigilanza**

### **4.1 Identificazione dell'Organismo di Vigilanza**

In base alle previsioni dell'art. 6, comma 1, lett. a) e b) del Decreto, la società può essere esonerata dalla responsabilità conseguente alla commissione di illeciti da parte dei soggetti qualificati ex art. 5 del Decreto, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello adottato e di curarne l'aggiornamento ad un organismo della società dotato di autonomi poteri di iniziativa e controllo.

L'affidamento a tale organismo dei suddetti compiti, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità prevista dal Decreto.

### **4.2 Caratteristiche dell'Organismo di Vigilanza**

Il compito di vigilare sul funzionamento, l'aggiornamento e la concreta applicazione del Modello è affidato ad un organismo dotato delle seguenti caratteristiche:

- indipendenza ed autonomia dai vertici, al fine di garantire l'imparzialità e la possibilità di operare anche quando esso sia chiamato a vigilare sull'applicazione del Modello da parte del vertice;
- professionalità, per garantirne le capacità di azione in un contesto che richiede spiccate doti di valutazione e di gestione dei rischi, di analisi delle procedure, di organizzazione aziendale, di finanza, di diritto;
- continuità di azione, al fine di garantire la costante attività di monitoraggio e di aggiornamento del Modello e la sua variazione al mutare delle condizioni aziendali di riferimento.

### **4.3 Composizione**

In assenza di riferimenti normativi, la concreta costituzione dell'Organismo di Vigilanza, che di fatto esercita un potere, da un lato, di prevenzione e, dall'altro, di controllo e intervento, è rimessa all'iniziativa organizzativa della società, sempre in funzione del quadro delineato dal Decreto.

In ottemperanza, quindi, a quanto stabilito dall'art. 6, comma 1, lett. b) del Decreto il Rappresentante Generale e l'Organo Amministrativo delle Società del Gruppo hanno optato per una composizione che, tenuto conto delle finalità perseguite dalla legge, è in grado di assicurare, in relazione alle proprie dimensioni ed alla propria complessità organizzativa, l'effettività dei controlli cui tale organismo è preposto e ha identificato il proprio Organismo di Vigilanza in un organismo collegiale, che riferisce al Rappresentante Generale / Organo Amministrativo delle Società del Gruppo sul proprio operato.

La scelta di un organismo collegiale è stata effettuata alla luce del progressivo ampliamento delle fattispecie penalistiche che possono coinvolgere direttamente la responsabilità amministrativa, al fine di offrire una maggior garanzia di prevenzione dei reati ed un miglior presidio dei processi organizzativi e di controllo considerati necessari.

In considerazione dei criteri sopra citati, l'Organismo di Vigilanza collegiale dovrà essere composto da quattro componenti, aventi competenze di revisione interna, compliance e legale, che verranno coadiuvati da un esterno nel ruolo di un Presidente dell'Organismo stesso.

In particolare le funzioni facenti parte dell'Organismo sono le seguenti:

- Internal Audit di Capogruppo;
- Compliance di Capogruppo;
- Legale di Capogruppo.

La scelta operata è ispirata al principio di nominare quali componenti l'Organismo coloro i quali, nell'ambito della struttura organizzativa e societaria, abbiano un ruolo che garantisca il miglior contributo allo svolgimento delle funzioni ed al perseguimento degli obiettivi dell'Organismo di Vigilanza ed è motivata anche in ragione dei requisiti di autonomia, indipendenza, professionalità e continuità di azione, richiesti dalla citata norma, proprie delle figure individuate.

E' facoltà dell'Organismo di nominare un segretario, scegliendolo anche al di fuori dei suoi componenti.

#### **4.4 Nomina, revoca e sostituzione**

La nomina di ogni componente dell'Organismo di Vigilanza è attribuita al Rappresentante Generale della Capogruppo ed ai singoli Organi Amministrativi delle Società del Gruppo, i quali nominano sulla base dei criteri enunciati.

Il Presidente dell'Organismo è nominato e revocato dal Rappresentante Generale per la Capogruppo e dai singoli Organi Amministrativi delle Società del Gruppo; in mancanza viene eletto dal medesimo Organismo di Vigilanza.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza dei requisiti soggettivi di eleggibilità. Il Rappresentante Generale della Capogruppo e i singoli Organi Amministrativi delle Società del Gruppo, in sede di nomina, devono dare atto della sussistenza dei requisiti di indipendenza, autonomia, onorabilità e professionalità dei componenti dell'Organismo di Vigilanza.

I componenti dell'Organismo devono essere in possesso di particolari "requisiti soggettivi" in funzione dello svolgimento della responsabilità affidata. Gli stessi devono attestare, facendone apposita dichiarazione all'atto della nomina e annualmente, l'assenza di cause di "incompatibilità", a titolo esemplificativo, di:

- non essere componenti dell'organo decisionale o direttori generali o componenti della società di revisione esterna o revisori incaricati da questa;
- non avere relazioni di coniugio, parentela o affinità entro il 4° grado incluso con componenti dell'organo decisionale o direttori generali della società o della società di revisione esterna o con revisori incaricati dalla società di revisione esterna né avere le suddette relazioni tra di loro;
- non essere portatori di conflitti di interesse, anche potenziali, tali da pregiudicare la loro indipendenza né di coincidenze di interesse esorbitanti da quella ordinaria che trova fondamento nel rapporto di dipendenza e nella relativa fidelizzazione o nel rapporto di prestazione d'opera intellettuale;
- non avere svolto, almeno nei tre esercizi precedenti l'attribuzione dell'incarico, funzioni di amministrazione, direzione o controllo in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate ovvero in imprese operanti nel settore creditizio, finanziario, mobiliare e assicurativo sottoposte a procedura di amministrazione straordinaria o

di funzioni di amministrazione o di componente dell'Organismo di Vigilanza di enti sottoposti alle sanzioni di cui al d. lgs. n. 231/2001;

- sentenza di condanna, anche non passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento), in Italia o all'estero, per i delitti richiamati dal d. lgs. n. 231/2001 od altri delitti comunque incidenti sulla moralità professionale, incluso il caso in cui sia stato concesso il beneficio della sospensione condizionale della pena; non essere stati sottoposti a misure di prevenzione disposte dall'Autorità Giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423, o della legge 31 maggio 1965, n. 575, salvi gli effetti della riabilitazione;
- condanna, con sentenza, anche non passata in giudicato, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese, incluso il caso in cui sia stato concesso il beneficio della sospensione condizionale della pena;
- pendenza di un procedimento per l'applicazione di una misura di prevenzione di cui alla legge 27 dicembre 1956 n. 1423 e alla legge 31 maggio 1965 n. 575 ovvero pronuncia del decreto di sequestro ex art. 2- bis della legge 31 maggio 1965 n. 575 ovvero decreto di applicazione di una misura di prevenzione, sia essa personale che reale.

Nel caso di perdita dei "requisiti soggettivi" previsti nel Modello, i componenti dell'Organismo devono informare il Rappresentante Legale della Capogruppo / Organi Amministrativi delle Società del Gruppo al fine di procedere alla sostituzione.

Inoltre, chiunque venga a conoscenza della perdita dei "requisiti soggettivi" previsti per i componenti dell'Organismo è tenuto ad informare il Rappresentante Legale della Capogruppo / Organi Amministrativi delle Società del Gruppo al fine di procedere alla sostituzione.

I componenti dell'Organismo sono revocati immediatamente dal Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo in caso di perdita dei requisiti soggettivi sopra elencati, di negligenza o mala fede nell'espletamento dei compiti connessi con l'incarico, o qualora sia ravvisabile altra "giusta causa" di revoca. In caso di revoca, il Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo provvedono tempestivamente alla sostituzione del componente revocato.

In caso di dimissione di uno o più componenti, il Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo procedono senza indugio a nominare uno o più sostituti.

L'Organismo decade per la revoca o le dimissioni di tutti i suoi componenti. In tal caso il Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo provvedono, senza indugio, alla sua ricostituzione.

L'Organismo di Vigilanza, per garantire l'efficace esercizio della sua funzione e la continuità della sua azione, deve essere titolare di una propria autonoma disponibilità di spesa, rapportata ad ipotesi di interventi straordinari e urgenti, da definire di volta in volta e da effettuare in maniera riservata, alla stregua delle esperienze e delle esigenze ordinariamente prevedibili per lo specifico organismo.

#### **4.5 Funzionamento**

Al fine di garantire piena autonomia all'Organismo, il Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo hanno considerato opportuno che le regole di funzionamento interno dell'Organismo (convocazioni, adunanze, quorum, modalità di gestione delle attività) vengano adottate direttamente dall'Organismo stesso, e formalizzate all'interno di un regolamento.

#### **4.6 Funzioni e poteri**

Il Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo, in coerenza con i principi sanciti dal d. lgs. n. 231/01, affidano all'Organismo i seguenti compiti e poteri:

- valutare il funzionamento e l'effettiva adeguatezza del Modello a prevenire la commissione degli illeciti sanzionati ai sensi del d. lgs. n. 231/2001;
- curare l'aggiornamento del Modello anche in relazione alle modifiche normative, agli orientamenti giurisprudenziali ed ai mutamenti organizzativi;
- elaborare un programma di verifica, in coerenza con i principi contenuti nel Modello, nell'ambito dei vari settori di attività, assicurandone l'attuazione;
- vigilare sull'osservanza del Modello da parte dei dipendenti, degli organi sociali e, nei limiti delle attività svolte, degli intermediari, dei fornitori e dei consulenti;
- effettuare proposte e osservazioni alle funzioni competenti per l'adozione delle opportune disposizioni interne, procedure e protocolli;
- mantenere i rapporti e assicurare flussi informativi verso il Rappresentante Generale della Capogruppo o gli Organi Amministrativi delle Società del Gruppo e garantendo un adeguato collegamento con la società di revisione esterna, nonché con gli altri organi di controllo;
- richiedere e acquisire informazioni e documentazione di ogni tipo da e verso ogni livello e settore, compiendo verifiche ed ispezioni al fine di accertare eventuali violazioni del Modello;
- assicurare l'elaborazione della reportistica sulle risultanze degli interventi effettuati;
- definire e promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché della formazione dei dipendenti e della sensibilizzazione degli stessi all'osservanza dei principi contenuti nel Modello;
- predisporre un efficace sistema di comunicazione interna per consentire la trasmissione e raccolta di notizie rilevanti ai fini del d. lgs. n. 231/2001, garantendo la tutela e riservatezza del segnalante;
- formulare previsioni di spesa per lo svolgimento della propria attività;
- promuovere l'attivazione di eventuali procedimenti disciplinari, supportando, altresì, la funzione competente anche in ordine alla valutazione circa l'adozione di eventuali sanzioni o provvedimenti.

#### **4.7 Modalità di interazione con le altre funzioni aziendali**

L'Organismo di Vigilanza, nello svolgimento dei compiti affidati e per proprie finalità istituzionali, potrà avvalersi in particolare della collaborazione di:

- l'Internal Audit, per la verifica dei processi gestionali e delle procedure organizzative emanate in attuazione del Modello;
- il Risk Management, per le attività di identificazione, valutazione e controllo dei rischi di commissione degli illeciti sanzionati ai sensi del d. lgs. n. 231/2001;
- Compliance, per l'identificazione dei nuovi illeciti sanzionati ai sensi del d. lgs. n. 231/2001 e l'analisi del loro possibile impatto, per la valutazione dell'adeguatezza ed efficacia delle misure organizzative adottate a prevenzione della commissione di tali illeciti, nonché per il supporto gestionale all'esercizio delle funzioni istituzionali dell'Organismo;
- di altre unità organizzative, quali, a mero titolo esemplificativo:

- Segreteria societaria (in ordine, ad esempio, ai flussi informativi agli organi sociali);
  - Risorse Umane (in ordine, ad esempio, alla formazione del personale ed ai procedimenti disciplinari);
  - l'Amministrazione Finanziaria (in ordine, ad esempio, al controllo dei flussi finanziari)
- di opportuni supporti esterni, secondo le valutazioni del caso.

E' previsto, inoltre, per il corretto e completo espletamento delle attività di vigilanza, un coordinamento sistematico dell'Organismo di Vigilanza con tutte le Direzioni aziendali.

Affinché l'Organismo di Vigilanza possa avere la massima efficacia operativa deve essere garantito l'accesso senza restrizioni a tutte le informazioni aziendali che lo stesso reputi rilevanti alla sua attività e, più in generale, a tutte le informazioni aziendali.

#### **4.8 La gestione delle segnalazioni**

Tutti i collaboratori interni ed esterni delle Società del Gruppo sono tenuti a riferire tempestivamente:

- qualsiasi azione o omissione ritenuta, in buona fede, non conforme al Modello;
- qualsiasi circostanza che abbia fatto ritenere, in buona fede, la sussistenza di un pericolo di reato.

La segnalazione può avvenire contattando direttamente l'Organismo di Vigilanza, secondo le modalità che esso avrà cura di specificare e comunicare a tutti i dipendenti attraverso l'indirizzo e-mail "odv231@helvetia.it".

I segnalanti in buona fede sono tutelati contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso è assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti delle Società del Gruppo o delle persone accusate erroneamente e/o in mala fede.

#### **4.9 Flusso di informazioni verso l'Organismo di Vigilanza**

Oltre alle citate segnalazioni relative a violazioni di carattere generale sopra descritte, le funzioni aziendali che operano nell'ambito di attività sensibili devono trasmettere all'Organismo di Vigilanza le informazioni concernenti:

- le risultanze periodiche dell'attività di controllo poste in essere per dare attuazione al Modello (quali, ad esempio, report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.);
- le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

#### **4.10 Reporting dell'Organismo di Vigilanza**

Le linee di reporting dell'Organismo di Vigilanza sono dirette verso il Rappresentante Generale della Capogruppo, gli Organi Amministrativi delle Società del Gruppo.

Il Rappresentante Generale della Capogruppo informa periodicamente il Board of Directors di Casamadre seguendo le procedure interne.

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi. Sono previste due linee di reporting; relativamente l'Organismo di Vigilanza:

- riferisce direttamente ed in via continuativa, anche per il tramite del proprio Presidente o di altro componente designato dallo stesso Organismo;
- trasmette, con cadenza almeno trimestrale ed annualmente entro 90 giorni dalla chiusura di ciascun esercizio, una relazione sulle attività svolte, segnalando ogni eventuale carenza o violazione riscontrata. Tale relazione comprende le proposte di aggiornamento del Modello, laddove se ne riscontri l'esigenza in relazione a mutate condizioni aziendali o variazioni del quadro normativo.

Potrà essere richiesta la convocazione dell'Organismo per riferire sul funzionamento del Modello o su situazioni specifiche, da parte dei suddetti organi.

#### **4.11 I controlli dell'Organismo di Vigilanza**

L'Organismo di Vigilanza deve esercitare le prescritte verifiche sul Modello e sulla sua attuazione. Da un punto di vista operativo, tali responsabilità si traducono nelle seguenti attività esemplificative:

- predisporre una lista dei dati e delle informazioni minime che devono essergli trasmesse o tenute a sua disposizione;
- svolgere funzioni di coordinamento e di impulso delle attività di verifica, proponendo l'aggiornamento del Modello in relazione alle esigenze che si dovessero manifestare;
- promuovere iniziative per la diffusione e la conoscenza del Modello nei confronti dei dipendenti e dei terzi con cui le Società del Gruppo hanno rapporti di natura contrattuale (agenti, collaboratori, partner commerciali, professionisti, consorzi, associazioni di imprese, joint venture, ...);
- interagire con le funzioni aziendali per gli aspetti attinenti l'applicazione del Modello (formazione del personale, provvedimenti disciplinari, ...) e per un migliore monitoraggio delle aree sensibili;
- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto dal Modello;
- raccogliere, elaborare, conservare dati ed informazioni relativi all'osservanza del Modello;
- condurre verifiche interne ed esterne volte ad accertare presunte violazioni del Modello.

Con le finalità sopra indicate, l'Organismo di Vigilanza ha, tra l'altro, il compito di:

- verificare periodicamente, con il supporto e la collaborazione delle funzioni competenti:
  - il rispetto delle procedure interne, anche quelle adottate nel corso di eventuali ispezioni compiute da funzionari della Pubblica Amministrazione o di Autorità di Vigilanza;
  - le deleghe dei poteri in vigore, prescrivendo eventualmente le modifiche necessarie;
  - la predisposizione di clausole standard dei documenti aventi valore contrattuale finalizzate all'osservanza delle disposizioni del Decreto, alla possibilità di effettuare azioni di controllo nei confronti dei destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute e all'attuazione di sanzioni (quali la risoluzione del contratto nei riguardi di partner o collaboratori esterni) qualora si accertino violazioni delle prescrizioni;

- con riferimento al bilancio, alle relazioni ed alle altre comunicazioni sociali previste dalla legge esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente o soggetto esterno e ad effettuare degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
- definire ed aggiornare le regole di comportamento delineate dal Modello, emanando anche linee guida e circolari interne se lo ritiene opportuno e/o necessario;
- indicare al management le opportune integrazioni ai sistemi gestionali delle risorse finanziarie (sia in entrata che in uscita), con l'introduzione di indicatori che permettano di rilevare anomalie nell'andamento dei flussi finanziari (flussi atipici e/o connotati da rilevanti margini di discrezionalità);
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, dall'Autorità di Vigilanza e da qualsiasi dipendente o soggetto esterno ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Ai sensi dell'art. 52 (Organi di controllo) del d. lgs. 21 novembre 2007, n. 231, l'Organismo di Vigilanza, unitamente a tutti i soggetti incaricati del controllo, comunque, è soggetto ad alcuni obblighi specifici:

- l'obbligo di vigilare sull'osservanza delle norme contenute nel decreto;
- specifici obblighi di comunicazione, a rilevanza sia meramente interna che esterna. In particolare questo deve:
  - a) comunicare, senza ritardo, alle Autorità di Vigilanza tutti gli atti o i fatti di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire una violazione delle disposizioni emanate ai sensi dell'art. 7, comma 2, del d. lgs. n. 231/2007;
  - b) comunicare, senza ritardo, al Rappresentante Generale o agli Organi Amministrativi delle Società del Gruppo, le infrazioni alle disposizioni di cui all'art. 41 d. lgs. n. 231/2007 di cui abbia notizia;
  - c) comunicare, entro trenta giorni, al Ministero dell'Economia e delle finanze infrazioni relative a (i) le limitazioni all'uso del contante e dei titoli al portatore e (ii) il divieto di conti e libretti di risparmio anonimi o con intestazione fittizia di cui ha notizia;
  - d) comunicare, entro trenta giorni, alla UIF le infrazioni agli obblighi di registrazione.

Il mancato rispetto degli obblighi di comunicazione è espressamente sanzionato dalla previsione contenuta nell'art. 55, comma quinto, del d. lgs. 231/2007, che recita: "*Chi, essendovi tenuto, omette di effettuare la comunicazione di cui all'art. 52, comma 2, è punito con la reclusione fino a un anno e con la multa da 100 a 1.000 euro*".

#### **4.12 Raccolta e conservazione delle informazioni**

L'Organismo di Vigilanza è tenuto a conservare in un apposito archivio (informatico o cartaceo) ogni informazione, segnalazione, report, relazione previsti nel Modello.

## **5. Il sistema disciplinare e sanzionatorio**

### **5.1 Disciplina sanzionatoria**

Il Decreto richiede che il Modello introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

Il sistema disciplinare previsto nei confronti dei dipendenti viene costantemente monitorato dalle Risorse Umane.

Poiché l'applicazione delle sanzioni è correlata unicamente al mancato rispetto delle misure definite nel Modello, essa prescinde dall'instaurazione o dall'esito di un eventuale procedimento penale instaurato contro chi abbia tenuto un comportamento contro le previsioni del Modello.

Il Modello prevede delle misure sanzionatorie anche nei confronti dei soggetti non dipendenti, che collaborano con le Società del Gruppo.

### **5.2 Accertamento della violazione**

Per quanto riguarda l'accertamento del mancato rispetto delle prescrizioni del Modello, lo svolgimento delle procedure disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti delle rispettive competenze.

L'Organismo di Vigilanza, nell'accertamento di violazioni del Modello, provvede a coinvolgere le Risorse Umane per la valutazione delle sanzioni previste.

L'Organismo di Vigilanza è tenuto a fornire il proprio parere in ordine alla eventuale archiviazione del procedimento disciplinare o alla applicazione della sanzione.

E' compito dell'Organismo di Vigilanza informare tempestivamente il Rappresentante Generale della Capogruppo, gli Organi Amministrativi delle Società del Gruppo e l'Internal Audit delle procedure di accertamento avviate e del loro esito.

Nei confronti dei dipendenti (impiegati, funzionari e dirigenti) che si rendano responsabili di violazioni alle prescrizioni fissate nel Modello relativamente alle procedure interne ed al comportamento che gli stessi sono tenuti a seguire nell'espletamento delle rispettive mansioni verranno applicate, nel rispetto dell'art. 7, L. 30 maggio 1970 n. 300 e delle normative speciali eventualmente applicabili, le sanzioni previste dal Codice Civile, dai vigenti:

- Contratto Collettivo Nazionale per la disciplina dei rapporti del personale dipendente non dirigente del settore assicurativo;
- Contratto Nazionale normativo ed economico per i dirigenti del settore assicurativo.

### **5.3 Misure nei confronti dei dipendenti non dirigenti**

Le sanzioni irrogabili nei confronti dei lavoratori dipendenti, conformemente a quanto previsto dall'articolo 7 della legge 30 maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) ed eventuali normative speciali applicabili, sono quelle previste dalle norme di contratto collettivo specificamente dedicate ai provvedimenti disciplinari. Si riporta come esemplificativo:

- rimprovero verbale;
- biasimo inflitto per iscritto;
- sospensione dal servizio e dal trattamento retributivo (per un periodo non superiore a dieci giorni);

- risoluzione del rapporto di lavoro per giustificato motivo;
- risoluzione del rapporto di lavoro per giusta causa.

Nella determinazione della sanzione e della sua entità si terrà conto:

- della intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia in relazione alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore, nel corso del rapporto di lavoro intercorso, riguardo alla sussistenza o meno di precedenti provvedimenti disciplinari adottati a carico del medesimo;
- delle concrete mansioni espletate dal lavoratore;
- della posizione funzionale delle persone concorrenti nei fatti costituenti la violazione disciplinare contestata;
- di ogni altra particolare circostanza che accompagni la violazione disciplinare contestata.

#### **5.4 Misure nei confronti dei dipendenti dirigenti**

In caso di violazione, da parte di Dirigenti, delle singole disposizioni e delle regole comportamentali contenute nel Modello, si applicheranno nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dalle norme di legge e di contratto..

#### **5.5 Misure nei confronti dei collaboratori esterni, intermediari e dei partner commerciali**

Al fine di favorire il rispetto da parte di collaboratori esterni, intermediari e partner commerciali, con cui si abbia una qualunque forma di collaborazione contrattualmente regolata, ove destinati a cooperare nell'ambito di attività sensibili, si provvede ad inserire, nei relativi contratti, clausole standard che impegnino contrattualmente tali soggetti a non adottare atti o comportamenti che potrebbero determinare la commissione, anche tentata, dei reati contemplati dal Decreto e ad adottare e attuare, ove necessario, procedure idonee a prevenire dette violazioni.

L'adozione di un atto o di uno dei comportamenti sopra citati sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali che saranno inserite nei relativi contratti che potranno prevedere, a titolo meramente esemplificativo, la facoltà di risoluzione del contratto e/o il pagamento di penali.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

#### **5.6 Misure nei confronti del Rappresentante Generale o degli Amministratori**

Ove da verifiche emergessero violazioni o tentativi di violazione del Modello riconducibili al Rappresentante Generale o agli Amministratori delle Società del Gruppo, l'Organismo di Vigilanza ne darà notizia rispettivamente al Board of Directors di Casamadre o agli Organi Amministrativi delle Società del Gruppo, affinché si provveda ad assumere, ciascuno per le proprie rispettive competenze, le iniziative previste dalla vigente normativa.

## Parte Speciale

La Parte Speciale contiene i risultati dell'analisi normativa, l'identificazione delle attività sensibili e dei presidi di controllo.

### 1. Reati contro la Pubblica Amministrazione

La presente Parte Speciale descrive e illustra regole di condotta e controlli che tutti i Destinatari del Modello adottano ed applicano al fine di prevenire il verificarsi dei reati rilevanti ai sensi degli articoli 24 e 25 del Decreto di seguito individuati.

La Parte Speciale è in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive.

#### 1.1 Analisi delle fattispecie di reato

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi dell'art. 24 e dell'art. 25 del Decreto, riportiamo qui di seguito una descrizione, in forma sintetica, dei reati alla cui commissione da parte di soggetti riconducibili all'ente (ai sensi dell'art. 5 del Decreto) è collegato il regime di responsabilità a carico dello stesso ente:

##### Malversazione a danno dello Stato o dell'Unione Europea (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 dell'Unione Europea, non si proceda all'utilizzo delle somme per gli scopi cui sono state ottenute.

Il reato stesso si configura anche per finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati;

##### Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)

Tale ipotesi di reato si configura nel caso 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 dall'Unione Europea.

In questo caso, contrariamente a quanto avviene per il reato di malversazione, non rileva l'uso che venga fatto delle erogazioni poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti;

##### 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 sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovute.

Questo reato potrebbe ravvisarsi nell'ipotesi in cui un collaboratore dell'ente (ad esempio, un dipendente o un agente) concorra nel reato del pubblico ufficiale, il quale approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per l'ente);

##### Corruzione per un atto d'ufficio o corruzione per un atto contrario ai doveri d'ufficio (artt. 318 - 319-bis c.p.)

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

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

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un reciproco vantaggio mentre nella concussione il concusso subisce la condotta del pubblico ufficiale e o dell'incaricato del pubblico servizio (concussi);

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

Tale ipotesi di reato si configura al fine di favorire o danneggiare una parte in un processo ci sia la corruzione di un pubblico ufficiale (non solo un magistrato ma anche un cancelliere o altro funzionario);

Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)

Soggetto attivo del reato previsto dalla norma in esame può essere:

- per la corruzione finalizzata al compimento di un atto d'ufficio (c.d. propria, prevista dall'art. 318 c.p.), solo l'incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato ;
- per la corruzione finalizzata ad un atto contrario ai doveri di ufficio (c.d. impropria, di cui all'art. 319 c.p.), ogni incaricato di un pubblico servizio .

Delitti del corruttore (art. 321 c.p.)

Le pene stabilite in relazione all'ipotesi di corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318 e 319 c.p.), si applicano anche, per disposizione della norma qui in esame, a chi dà o promette al pubblico ufficiale (art. 357 c.p.) o all'incaricato di un pubblico servizio (art. 358 c.p.) il denaro o altra utilità.

In altri termini, colui che corrompe commette una autonoma fattispecie di reato rispetto a quella compiuta dal pubblico ufficiale (o incaricato di pubblico servizio) che si è lasciato corrompere;

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 rifiuti l'offerta illecitamente avanzategli;

Concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e degli Stati esteri (art. 322-bis c.p.)

Le disposizioni degli artt. 317 - 320 e 322, comma 3 e 4, c.p., si applicano anche a membri delle Istituzioni comunitarie europee, nonché ai funzionari delle stesse e dell'intera struttura amministrativa comunitaria, e alle persone comandate presso la Comunità con particolari funzioni o addette ad enti previsti dai trattati e alle persone che nell'ambito degli Stati membri dell'Unione europea svolgono attività corrispondenti a quelle che nel nostro ordinamento sono svolte da pubblici ufficiali o da incaricati di un pubblico servizio (cfr. artt. 357 e ss. c.p.).

Ciò premesso, va detto che l'art. 322-bis c.p. incrimina altresì – e questo è d'interesse per i privati che abbiano a che fare con i soggetti sopra elencati – tutti coloro che compiano le attività colpite dagli artt. 321 e 322 c.p. (cioè attività corruttive) nei confronti delle persone medesime. Di più l'art. 322-bis c.p. incrimina anche l'offerta o promessa di denaro o altra utilità “a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri [diversi da quelli dell'Unione Europea] o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o altri un indebito vantaggio in operazioni economiche internazionali”;

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 siano posti in essere artifici o raggiri per indurre in errore e arrecare danno all'ente pubblico per realizzare un ingiusto profitto come, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio 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 in danno dello Stato, di altro Ente Pubblico (art. 640-ter c.p.)

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

Può integrarsi il reato 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.

## 1.2 Attività sensibili

Le analisi svolte hanno permesso di individuare le attività sensibili descritte di seguito.

**Negoziazione, stipulazione, esecuzione contratti o convenzioni con pubbliche amministrazioni mediante procedure negoziate (affidamento o trattativa privata).**

Attività di negoziazione/stipulazione/esecuzione di contratti e/o convenzioni con Pubbliche Amministrazioni, con dipendenti di Pubbliche Amministrazioni (nell'ambito di un rapporto privatistico - "privati sensibili") e altri contratti con Pubbliche Amministrazioni (es. consulenze, locazione o vendite di beni, ecc.) mediante procedure negoziate, anche a livello comunitario.

**Negoziazione, stipulazione ed esecuzione contratti o convenzioni con pubbliche amministrazioni ai quali si perviene mediante procedure ad evidenza pubblica (aperte o ristrette).**

Attività di negoziazione/stipulazione/esecuzione di contratti e/o convenzioni con Pubbliche Amministrazioni e altri contratti con Pubbliche Amministrazioni (es. consulenze, locazione o vendite di beni, ecc.) mediante partecipazione a procedure di gara, indette da Pubbliche Amministrazioni o a similari procedure svolte in contesto competitivo (anche a livello comunitario).

**Liquidazione sinistri a favore o per conto di pubbliche amministrazioni**

Liquidazioni a favore di Pubbliche Amministrazioni, liquidazioni per conto di Pubbliche Amministrazioni, liquidazioni a favore di dipendenti di Pubbliche Amministrazioni (in relazione ad un contratto stipulato / negoziato / gestito da una Pubblica Amministrazione), liquidazioni a favore di dipendente di Pubblica Amministrazione (nell'ambito di un rapporto esclusivamente privatistico - "privati sensibili").

**Gestione dei contenziosi giudiziali e stragiudiziali con personale dipendente ed ex dipendente e collaboratori esterni.**

Si tratta dell'attività relativa alla gestione di contenziosi giudiziali e stragiudiziali che coinvolgono l'ente, nonché della selezione, valutazione e remunerazione dei consulenti legali esterni con riferimento a qualunque tipologia di vertenza, escluso l'ambito della liquidazione tecnica (cause di lavoro, vertenze tributarie, contenzioso societario, ecc.).

**Gestione dei contenziosi giudiziari e stragiudiziali con la clientela.**

Si tratta dell'attività relativa alla gestione di contenziosi giudiziari e stragiudiziali che coinvolgono l'ente, nonché della selezione, valutazione e remunerazione dei consulenti legali esterni con riferimento a qualunque tipologia di vertenza relativa o alla attività di liquidazione tecniche danni e vita o alle attività assuntive.

**Gestione dei rapporti con la pubblica amministrazione per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (D.Lgs.e successive modificazioni/integrazioni)**

Si tratta della gestione delle verifiche/ispezioni in materia di sicurezza e igiene sul lavoro svolte dalle autorità competenti e della cura dei relativi adempimenti.

**Amministrazione e gestione del personale**

Si tratta delle attività di selezione, assunzione, valutazione, formazione e sviluppo del personale, di amministrazione degli aspetti retributivi e previdenziali connessi al personale dipendente e ai collaboratori esterni.

**Rapporti con enti previdenziali e assistenziali**

Gestione dei rapporti con enti previdenziali ed assistenziali (INPS, INAIL, ecc.) anche in occasione di verifiche/ispezioni in materia svolte dalle autorità competenti e della cura dei relativi adempimenti, inclusi quelli aventi ad oggetto l'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata.

**Rapporti con Autorità di Vigilanza relativi allo svolgimento di attività regolate dalla normativa di riferimento e gestione dei rapporti per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali.**

Si tratta della gestione dei rapporti ordinari e continuativi con l'Autorità di Vigilanza, anche in caso di ispezioni e della gestione dell'attività di richiesta e ottenimento di provvedimenti amministrativi occasionali necessari allo svolgimento di attività strumentali a quelle tipiche aziendali.

**Gestione dei rapporti con l'amministrazione finanziaria**

Si tratta della gestione dei rapporti con l'Amministrazione Finanziaria, anche in occasione di accertamenti/verifiche/ispezioni nonché in occasione di eventuali procedimenti di interpello.

**Promozioni commerciali e sponsorizzazioni a pubbliche amministrazioni.**

Si tratta della gestione delle richieste e dei contratti di sponsorizzazione per la realizzazione di restauri di immobili di interesse storico/artistico e per la realizzazione di iniziative di carattere culturale, sportivo, ecc. patrocinate da Enti Pubblici.

**Acquisizione e/o gestione di contributi, sovvenzioni e finanziamenti concessi da pubbliche amministrazioni.**

Si tratta della gestione delle richieste e di contributi e sovvenzioni da Pubbliche Amministrazioni.

**Ogni possibilità di detenere, maneggiare o utilizzare denaro/valori di bollo, disponibilità di fondi**

Disponibilità di fondi liquidi (piccola cassa) e detenzione di valori bollati.

**Gestione di software di pubbliche amministrazioni o forniti da terzi per conto di pubbliche amministrazioni e collegamenti telematici (in entrata/uscita) o trasmissione di dati su supporti informatici a pubbliche amministrazioni, enti pubblici o autorità**

Gestione di applicativi software forniti da Pubbliche Amministrazioni. Il reato consiste nell'alterazione di registri informatici della Pubblica Amministrazione (ad es. per fare risultare esistenti condizioni essenziali per la partecipazione a gare ovvero per la successiva produzione

di documenti attestanti fatti o circostanze inesistenti o per modificare dati di interesse dell'azienda già trasmessi alla Pubblica Amministrazione).

### **1.3 Sistema dei controlli**

Il sistema di controlli applicabili alle sopra indicate attività sensibili è stato definito utilizzando, come riferimento, le Linee Guida ad oggi pubblicate dalle principali associazioni di categoria nonché le *best practice* internazionali in tema di rischi di frode e corruzione.

Il Modello prevede l'applicazione di:

- Controlli generali: controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili.

#### **1.3.1 Controlli generali**

Il Modello contempla l'applicazione dei seguenti controlli generali:

##### Segregazione delle attività/funzioni/processo

Si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza in particolare, nei rapporti che l'ente intrattiene con la Pubblica Amministrazione.

##### Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Le disposizioni aziendali devono fornire chiari principi generali di riferimento per la regolamentazione dell'attività.

La società provvede alla definizione, alla manutenzione e alla pubblicazione nella Intranet aziendale di tutte le procedure interne, ivi incluse quelle da seguire per la formazione e l'attuazione delle decisioni della società.

##### Sistema deleghe, poteri di firma e poteri autorizzativi:

Si prevede l'obbligo di fissare costantemente ed aggiornare regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma.

##### Tracciabilità

Si richiede l'esistenza di presidi che, in relazione ad ogni comunicazione scritta relativa ai rapporti con la Pubblica Amministrazione in merito a ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

#### **1.3.2 Controlli specifici**

Di seguito si individuano gli standard minimi di controllo specificatamente individuati per aree di attività dell'ente che includono le attività sensibili sopra individuate:

##### Obbligo di segnalazione

Deve essere segnalato l'avvio e le fasi più significative di un procedimento o di un rapporto, anche in via mediata, nell'esercizio dell'attività sia ordinaria sia straordinaria, con la Pubblica Amministrazione (partecipazione a procedure di gara o di negoziazione diretta, richiesta di finanziamenti pubblici da parte di organismi nazionali o esteri, ...), specificando la tipologia di operazione, le caratteristiche ed i soggetti esterni coinvolti, in particolar modo se si tratta di enti pubblici. La segnalazione deve contenere una sintetica descrizione delle caratteristiche del rapporto con la Pubblica Amministrazione specificando la tipologia di operazione, le sue caratteristiche ed i soggetti esterni coinvolti, in particolar modo se si tratta di enti pubblici. In ogni

caso la segnalazione deve essere conservata, al fine di consentire, in qualunque momento, l'effettuazione di controlli da parte del soggetto destinatario della segnalazione o dell'Organismo di Vigilanza.

#### Autorizzazione formale

Deve esistere un'autorizzazione formalizzata alla stipulazione di un atto formale o all'esecuzione di una operazione.

#### Report

Devono esistere report inviati al superiore gerarchico o al referente interno individuato, dettagliati per ogni singola operazione.

#### Registrazione

L'operazione deve essere registrata e documentata come da procedure aziendali.

#### Sicurezza informatica

Deve essere affidata esclusivamente a una Funzione competente, che ne deve assicurare la tracciabilità la cancellazione di dati, liste di controllo e archivi. Devono esistere liste di controllo degli accessi ai sistemi informativi e automatismi di segnalazione all'amministratore del sistema di operazioni non autorizzate: cancellazioni, tentativi di accesso, alterazione delle funzionalità del sistema. I responsabili del monitoraggio del sistema informatico aziendale e della sua revisione censiranno e verificheranno periodicamente:

- le persone che hanno accesso ai mezzi informatici, con particolare riferimento a quanti utilizzano mezzi destinati al contatto con l'esterno (trasmissione dei dati tramite comunicazioni telematiche o informatiche, in modo particolare se questi sono corredati di autenticazione o firma digitale, invio di file prodotti da elaborazioni on line o batch, ...);
- le procedure che producono i dati aziendali, con particolare riferimento a quelle che inviano informazioni aventi rilevanza all'esterno.

Rispetto alle prescrizioni del Modello, permane la validità delle disposizioni definite nelle procedure di maggiore tutela previste nell'ambito aziendale per lo svolgimento delle attività sensibili.

## 2. Reati societari

La presente Parte Speciale descrive e illustra regole di condotta e standard di controllo che tutti i Destinatari adottano ed applicano al fine di prevenire il verificarsi dei reati rilevanti ai sensi dell'art. 25-ter Decreto di seguito individuati.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari come sopra identificati nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### 2.1 Analisi delle fattispecie di reato

Di seguito vengono brevemente descritti i reati richiamati dall'art. 25-ter (Reati societari) del Decreto, così come modificato dalla legge 28 dicembre 2005 n. 262 (di seguito anche legge n. 262/2005).

E' opportuno evidenziare che, qualora si tratti di delitti, tali fattispecie sono punibili anche a titolo di tentativo, ai sensi dell'art. 56 c.p., e che un ulteriore ampliamento della punibilità è legato alla possibilità di concorrere consapevolmente con altri soggetti nella realizzazione delle fattispecie di reato (nell'ipotesi di concorso di più persone nella commissione di un reato, disciplinata dall'art. 110 c.p.), apportando quindi un contributo che può essere minore rispetto alla realizzazione integrale della fattispecie prevista dal legislatore.

I reati contemplati nel Decreto possono essere raggruppati nelle seguenti tipologie:

#### A. Falsità in comunicazioni, prospetti e relazioni

*False comunicazioni sociali (art. 2621 c.c., così come modificato dall'art 30, primo comma, della legge n. 262/2005) e false comunicazioni sociali in danno dell'ente, dei soci o dei creditori (art. 2622 c.c., così come modificato dall'art. 30, secondo comma, della legge n. 262/2005)*

La condotta consiste in una esposizione di informazioni non rispondenti al vero ancorché oggetto di valutazioni ovvero nell'omissione di informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria dell'ente o del gruppo al quale essa appartiene; deve essere tenuta con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto.

Soggetti attivi del reato possono essere solo gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori (trattasi, quindi, di cd. "reati propri"), nonché coloro che secondo l'art. 110 c.p. concorrono nel reato da questi ultimi commesso.

Le comunicazioni devono essere dirette "ai soci o al pubblico"; sono escluse dall'ambito applicativo della fattispecie in esame, le comunicazioni a destinatario individuale, quelle interorganiche e quelle rivolte ad autorità pubbliche di controllo.

Le informazioni rese o omesse devono essere tali da alterare in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria dell'ente o del gruppo al quale essa appartiene e devono essere oggettivamente idonee a indurre in errore i destinatari della comunicazione circa tale situazione.

La responsabilità si ravvisa anche nell'ipotesi in cui le informazioni false od omesse riguardino beni posseduti od amministrati dall'ente per conto di terzi.

La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria dell'ente o del gruppo al

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

In ogni caso il fatto non è punibile (e il superamento di tali soglie di rilevanza perde, comunque, rilievo penale) se è conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.

Con riferimento alle previsioni dell'art. 2622 c.c., si precisa, inoltre, che:

- la fattispecie delittuosa consta dell'ulteriore elemento del danno patrimoniale cagionato all'ente, ai soci o ai creditori;
- la pena è aumentata quando il fatto cagiona un grave nocumento ai risparmiatori. Il nocumento si considera grave quando abbia riguardato un numero di risparmiatori superiore allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT, ovvero se sia consistito nella distruzione o nella riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo;
- il reato è punibile a querela della parte lesa. Si procede a querela anche se il fatto integra altro delitto, ancorché aggravato, a danno del patrimonio di soggetti diversi dai soci e dai creditori, salvo che sia commesso in danno dello Stato, di altri enti pubblici o delle Comunità europee. Nel caso di enti soggetti alle disposizioni della parte IV, titolo III, capo II, del TUF, il delitto è procedibile d'ufficio.

#### Falso in prospetto (art. 173-bis TUF)

L'art. 34 (Falso in prospetto), comma 2, della legge n. 262/2005 ha abrogato l'art. 2623 del codice civile, che puniva il reato in esame e la fattispecie criminosa – in precedenza sanzionata ai sensi della norma abrogata - è, attualmente, prevista e sanzionata dall'art. 173-bis del TUF.

Si precisa, con riferimento ai reati presupposto della responsabilità amministrativa ex Decreto, che l'art. 25-ter del citato Decreto richiama, attualmente, la norma civilistica abrogata, mentre non fa riferimento alcuno al reato introdotto dalla legge n. 262/2005. Le novità legislative sembrerebbero, quindi, comportare il venir meno della responsabilità amministrativa dell'ente ai sensi dell'art. 25-ter del Decreto con riferimento al reato di falso in prospetto.

Si ritiene, in ogni caso opportuno, sia pure in difetto di un esplicito richiamo normativo in tal senso, sottoporre a particolare attenzione la predisposizione dei prospetti e dei documenti richiamati dall'art. 173-bis del TUF.

La condotta criminosa consiste nell'esporre, nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, false informazioni, che siano idonee ad indurre in errore i destinatari del prospetto; nell'occultamento, nei documenti sopra indicati, di dati o notizie in modo idoneo ad indurre in errore i destinatari dei medesimi.

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

La fattispecie si concretizza quando i responsabili della revisione, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o nelle altre comunicazioni, con l'intenzione di ingannare i destinatari delle comunicazioni stesse, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria dell'ente, in modo idoneo ad indurre in errore i destinatari delle suddette comunicazioni.

Soggetti attivi sono i responsabili della società di revisione, ma i componenti degli organi di amministrazione e di controllo e i dipendenti dell'ente revisionato possono essere coinvolti a titolo di concorso nel reato.

## **B. Tutela penale del capitale sociale**

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

Tale ipotesi di reato si configura nel caso in cui amministratori, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

In altri termini, viene incriminata una riduzione del capitale, con conseguente mancata ufficializzazione della riduzione del capitale reale tramite l'abbassamento del capitale nominale, il cui valore, pertanto, risulta superiore a quello del capitale reale. La condotta incriminata deve essere tenuta nei confronti dei soci e per integrare la fattispecie non occorre che tutti i soci siano liberati dall'obbligo di conferimento ma è sufficiente che lo sia un singolo socio o più soci.

Sotto un profilo astratto, sembra difficile che il reato possa essere commesso nell'interesse o a vantaggio dell'ente, implicando in tal modo una responsabilità mentre, nella pratica, potrebbe verificarsi in relazione ai rapporti infragruppo;

### *Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)*

Tale ipotesi di reato si configura nel caso in cui gli amministratori ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite. Con riferimento ad eventuali profili di rischio valgono, al riguardo, le osservazioni compiute con riferimento alla disposizione precedente, risultando anche in tale caso particolarmente problematici i profili di rilevanza della fattispecie in esame in relazione alle operazioni infragruppo;

### *Illecite operazioni sulle azioni o quote sociali o dell'ente controllante (art. 2628 c.c.)*

Tale ipotesi di reato si configura nel caso in cui gli amministratori, fuori dei casi consentiti dalla legge, acquistino o sottoscrivano azioni o quote sociali (anche dell'ente controllante), cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, in violazione delle disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altro ente scissioni, cagionando danno ai creditori;

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori e i soci conferenti, anche in parte, formino od aumentino fittiziamente il capitale dell'ente mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio dell'ente nel caso di trasformazione;

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

Tale ipotesi di reato si configura nel caso in cui i liquidatori, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionino danno ai creditori.

## **C. Tutela penale del regolare funzionamento dell'ente**

### *Impedito controllo (art. 2625 c.c.)*

Tale ipotesi di reato si configura nel caso in cui gli amministratori, occultando documenti o con altri idonei artifici, impediscano o comunque ostacolino lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione;

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

Tale ipotesi di reato si configura nel caso in cui chiunque, con atti simulati o fraudolenti (cioè con inganno e conseguente induzione in errore di taluno), determini la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

#### **D. Tutela penale contro le frodi**

*Aggiotaggio (art. 2637 c.c.)*

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale. Si tratta di un reato comune, cioè di un reato che può essere commesso da chiunque.

#### **E. Tutela penale delle funzioni di vigilanza**

*Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638 c.c.)*

Tale ipotesi di reato si configura nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori dell'ente e gli altri soggetti sottoposti per legge alle Autorità pubbliche di Vigilanza, o tenuti ad obblighi nei loro confronti, nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongano fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultino con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima.

#### **F. Interessi dell'amministratore**

*Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.)*

Il reato, introdotto dall'art. 31 della legge n. 262/2005, consiste nella violazione, da parte dell'amministratore o di un componente il consiglio di gestione, degli obblighi di comunicazione imposti dall'art. 2391, comma 1, c.c. , il quale prevede che si dia notizia agli amministratori e al Collegio Sindacale di ogni interesse, per conto proprio o di terzi, si abbia in una determinata operazione dell'ente se dalla violazione siano derivati danni all'ente o a terzi. Tale reato è, però, sanzionato ai fini del d. lgs. n. 231/2001 soltanto quando dal compimento dello stesso abbia tratto interesse o vantaggio l'ente.

Il reato è proprio: possono essere, quindi, soggetti attivi solo gli amministratori di enti con titoli quotati in mercati regolamentati italiani o comunitari o con titoli diffusi tra il pubblico in misura rilevante (ai sensi dell'art. 116 del TUF), di ente creditizio o finanziario.

Il dolo consiste nella coscienza e volontà dell'amministratore di non dare notizia circa interessi che egli, per conto proprio o di terzi, abbia in una operazione dell'ente o di non precisare natura, termini, origine e portata degli interessi stessi o anche di non astenersi dall'operazione se amministratore delegato o ancora di non darne notizia alla prima assemblea utile se amministratore unico.

## 2.2 Attività sensibili

In relazione ai reati ed alle condotte criminose sopra esplicitate, le attività sensibili risultano essere, con riferimento ai reati analizzati, ai fini del presente Modello, le seguenti:

**Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di autorità di vigilanza.**

Si tratta delle attività che riguarda le operazioni relative alla rilevazione, registrazione e rappresentazione dell'attività d'impresa nelle scritture contabili, nei bilanci, nelle relazioni e in qualsiasi altro prospetto relativo alla situazione economica, patrimoniale e finanziaria della dell'ente richiesto da disposizioni di legge e dell'attività e degli adempimenti legislativi legati alla tenuta dei registri contabili, di quelli assicurativi e dei libri sociali e della gestione dei rapporti con le autorità di vigilanza in merito agli adempimenti previsti in tema di comunicazioni dei dati societari.

**Predisposizione di prospetti relativi alla sollecitazione, all'investimento, al pubblico risparmio e/o di ammissione alla quotazione in mercati regolamentati e non regolamentati e/o operazioni straordinarie sul capitale (opa, opv, ops, ecc.)**

Predisposizione e diffusione di prospetti relativi a emissione di azioni. Predisposizione e diffusione di prospetti con fini di sollecitazione al pubblico risparmio. Predisposizione e diffusione di prospetti relativi a operazioni straordinarie sul capitale (opa, opv, ops).

**Gestione dei rapporti con la società di revisione e altri organi societari e relativa redazione, tenuta e conservazione dei documenti su cui gli stessi possono esercitare il controllo.**

Si tratta dell'attività di gestione dei rapporti con la società di revisione e i soci relativi alle attività di controllo da questi esercitate e della corretta gestione dei documenti sui quali tali soggetti possono esercitare il controllo sulla base della normativa vigente.

**Attività di preparazione delle riunioni assembleari. Attività di rilevanza societaria e adempimenti di oneri societari**

Si tratta degli adempimenti previsti in relazione alla preparazione delle riunioni assembleari, inclusa la documentazione oggetto dell'assemblea.

**Comunicazione degli interessi degli amministratori**

Si tratta degli adempimenti legati alla comunicazione, da parte degli amministratori, della presenza o dell'assenza di un interesse, proprio o di terzi, in operazioni della società .

**Gestione delle incombenze societarie; operazioni sul capitale e operazioni su azioni e quote**

Si tratta degli adempimenti legati alla gestione delle attività in oggetto al fine di salvaguardare il patrimonio della Società, nel caso di operazioni su azioni e quote o di acconti su dividendi, conferimenti, fusioni e scissioni.

Ad esse si aggiungono le attività di gestione delle comunicazione verso l'esterno riguardanti notizie o dati e di negoziazione di strumenti finanziari, sensibili con riferimento al reato di agiotaggio, analizzate con riferimento ai c.d. "Abusi di mercato".

## 2.3 Sistema dei controlli

Il sistema di controlli applicabili alle sopra indicate attività sensibili è stato definito utilizzando, come riferimento le Linee Guida ad oggi pubblicate dalle principali associazioni di categoria.

Il Modello prevede l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili.

### **2.3.1 Controlli generali**

Il controllo generale, valevole per tutte le attività sensibili individuate, è descritto di seguito.

#### Segregazione delle attività/funzioni/processo

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

### **2.3.2 Controlli specifici**

I controlli specificatamente individuati per aree di attività dell'ente che includono le attività sensibili come sopra individuate, sono descritti di seguito.

#### **Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di autorità di vigilanza.**

Oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

#### Normativa aziendale e circolari interne destinate a regolamentare la specifica attività: le disposizioni aziendali devono fornire chiari principi generali di riferimento per la regolamentazione dell'attività.

Con riferimento all'attività svolta dal personale coinvolto in attività di predisposizione del bilancio, lo standard prescrive che siano portate a conoscenza norme di gruppo che definiscono con chiarezza i principi contabili da adottare per la definizione delle poste del bilancio e le modalità operative per la loro contabilizzazione, tempestivamente aggiornate alla luce delle novità della normativa civilistica e diffuse ai destinatari sopra indicati.

#### Sistema deleghe, poteri di firma e poteri autorizzativi.

Devono esistere regole formalizzate e costantemente aggiornate per l'esercizio di poteri autorizzativi interni e poteri di firma.

#### Tracciabilità

Il sistema informatico utilizzato per la trasmissione di dati e informazioni deve garantire la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascuna funzione coinvolta nel processo deve garantire la tracciabilità delle informazioni contabili non generate in automatico dal sistema informatico. Lo standard richiede altresì che sia disciplinata la procedura di cancellazione dei dati e delle informazioni contabili.

#### Istruzioni di chiusura contabile

Devono esistere ed essere diffuse istruzioni rivolte alle diverse funzioni aziendali, che indichino dati e notizie che è necessario fornire alle funzioni responsabili del processo di redazione del bilancio in occasione delle chiusure annuali ed infrannuali, nonché le modalità e la tempistica di trasmissione degli stessi.

#### Conservazione dei documenti contabili obbligatori

Deve esistere una disposizione aziendale chiara e formalizzata che identifichi ruoli e responsabilità, relativamente alla tenuta, alla trascrizione e alla conservazione dei registri contabili, assicurativi e dei libri sociali nel rispetto delle disposizioni normative.

#### Attività di formazione

Devono essere svolte attività di formazione di base, rivolte a servizi coinvolti nella redazione del bilancio e degli altri documenti connessi, in merito alle principali nozioni ed alle problematiche giuridico-contabili inerenti il bilancio.

#### Sicurezza informatica

Devono esistere adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel d. lgs. n. 196/03 e nelle best practice internazionali.

#### **Predisposizione di prospetti relativi alla sollecitazione, all'investimento, al pubblico risparmio e/o di ammissione alla quotazione in mercati regolamentati e non regolamentati e/o operazioni straordinarie sul capitale (opa, opv, ops, ecc.)**

##### Flusso informativo/processo

Lo standard prescrive l'esistenza di una procedura formalizzata che preveda ruoli e responsabilità relativamente al flusso informativo da fornire alle funzioni coinvolte nel processo di formazione del bilancio di esercizio o di altre comunicazioni sociali.

##### Tracciabilità

Si richiede l'esistenza di presidi che, in relazione ad ogni comunicazione scritta che assicuri la tracciabilità degli elementi informativi e delle relative fonti.

##### Registrazione e archiviazione

La documentazione deve essere registrata e archiviata come da procedure aziendali.

#### **Gestione dei rapporti con la società di revisione, il collegio sindacale e altri organi societari e relativa redazione, tenuta e conservazione dei documenti su cui gli stessi possono esercitare il controllo.**

Oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

##### Tracciabilità

Deve essere assicurata la tracciabilità della documentazione e delle relative fonti e degli elementi informativi, nonché la relativa archiviazione.

##### Selezione della società di revisione e sua indipendenza nel mandato

Deve esistere una disposizione aziendale che regolamenti le fasi di selezione della società di revisione contabile e devono esistere regole per salvaguardare l'indipendenza della società di revisione aderenti alle disposizioni normative vigenti al fine di evitare che l'incarico sia affidato o permanga in capo a società di revisione che si trovino in una situazione di incompatibilità con l'ente.

##### Riunioni tra società di revisione, collegio sindacale e Organismo di Vigilanza

Devono essere effettuate una o più riunioni tra la società di revisione (qualora alla stessa sia stato affidato l'esercizio del controllo contabile) e l'Organismo di Vigilanza aventi ad oggetto la verifica sull'osservanza della disciplina prevista in tema di normativa societaria/corporate

governance nonché il rispetto dei comportamenti conseguenti da parte degli amministratori, del management e dei dipendenti.

#### Obbligo di informativa verso la Revisione Interna

L'Organismo di Vigilanza deve ricevere copia delle richieste di informazioni o documentazione provenienti dai soci, da organi sociali o dalla società di revisione (qualora alla stessa sia stato affidato l'esercizio del controllo contabile).

### **Attività di preparazione delle riunioni assembleari. Attività di rilevanza societaria e adempimenti di oneri societari**

Con riferimento a quest'attività sensibile gli standard di controllo specifici sono i seguenti:

#### Obblighi informativi

Deve essere effettuata almeno una riunione tra il Collegio Sindacale, la Società di Revisione e l'Organismo di Vigilanza aventi ad oggetto la verifica sull'osservanza della normativa societaria/corporate governance, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del management, dei dipendenti.

#### Regole per l'esercizio

Devono essere definite regole formalizzate per il controllo dell'esercizio del diritto di voto e per il controllo della raccolta ed esercizio delle deleghe di voto.

#### Gestione del verbale

Deve esistere una disposizione aziendale chiara e formalizzata che identifichi ruoli e responsabilità, relativamente alla trascrizione, pubblicazione del verbale d'assemblea e conservazione del libro delle adunanze e deliberazioni delle assemblee.

#### Dichiarazione in sede consiliare

Deve essere verificata in sede consiliare la presenza o l'assenza di un interesse, proprio o di terzi, degli amministratori nelle operazioni oggetto della riunione con evidenza nel relativo verbale.

### **Comunicazione degli interessi degli amministratori**

Con riferimento all'attività sensibile gli standard di controllo specifici sono i seguenti:

#### Comunicazioni in sede di accettazione della carica di amministratore

Deve esistere una disposizione aziendale che imponga, al momento dell'accettazione della carica, e successivamente con tempestività, a tutti gli Amministratori di comunicare alla società che amministrano:

- le eventuali ulteriori cariche ricoperte in altre società;
- le partecipazioni al capitale di altra società che abbia rapporti con la Società e l'interesse in qualsiasi tipo di operazione in cui controparte sia una società del Gruppo.

#### Criteri di indirizzo

Deve esistere una disposizione aziendale che contenga i criteri di indirizzo formalizzati e le modalità di condotta cui l'amministratore (che eventualmente operi in qualità di amministratore in altra società) dovrà attenersi, laddove sia ipotizzabile la sussistenza di interessi a norma dell'art. 2391 c.c.

#### Comunicazione degli interessi in una determinata operazione

Deve esistere una disposizione aziendale che disponga la richiesta preventiva a tutti i partecipanti alla riunione di un Consiglio di Amministrazione della Società ex art. 2629-bis c.c. di dichiarare, all'apertura della riunione, la sussistenza di interessi la cui comunicazione sia richiesta nelle forme prescritte dall'art. 2391, comma 1, c. c..

**Gestione delle incombenze societarie; operazioni sul capitale e operazioni su azioni e quote**

Con riferimento all'attività sensibile gli standard di controllo specifici sono i seguenti:

**Tracciabilità**

Si richiede l'esistenza di presidi che, in relazione ad ogni comunicazione scritta che assicuri la tracciabilità degli elementi informativi e delle relative fonti.

**Registrazione e archiviazione**

La documentazione deve essere registrata e archiviata come da procedure aziendali.

Rispetto alle prescrizioni del Modello, permane la validità delle disposizioni definite nelle procedure di maggiore tutela previste nell'ambito aziendale per lo svolgimento delle attività sensibili.

### **3. Gestione delle risorse economiche e finanziarie**

Con riferimento alle attività di gestione delle risorse finanziarie, anche in collegamento con quanto previsto dal Decreto all'art. 6, comma 2 lett. c), e delle risorse economiche da parte dei soggetti in posizione apicale, e in relazione ai reati ed alle condotte criminose esplicitate nelle precedenti Parti Speciali, sono state individuate alcune aree sensibili e definite norme e principi di comportamento, unitamente ai controlli diretti a verificarne il rispetto e l'attuazione.

#### **3.1 Attività sensibili**

L'analisi dei processi aziendali dell'ente ha consentito di individuare determinate aree sensibili Tali aree riguardano, in particolare modo:

##### **Gestione delle risorse finanziarie**

- l'attività di gestione dei flussi finanziari;
- la selezione e valutazione dei consulenti/agenti;
- l'assunzione del personale;
- la gestione degli omaggi e delle iniziative promozionali.

#### **3.2 Sistema dei controlli**

##### **3.2.1 Controlli generali**

Tali attività sono soggette, oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, a determinati standard di controllo.

L'elencazione individua uno standard minimo di comportamento e fa salve le eventuali procedure di controllo di maggiore tutela o più specifiche.

##### **Separazione delle responsabilità / funzioni / processo**

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

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

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione di:

- attività di gestione dei flussi finanziari che definisca, fra l'altro:
  - a) ruoli e responsabilità dei soggetti coinvolti;
  - b) pianificazione, da parte delle funzioni aziendali, del proprio fabbisogno finanziario e comunicazione dello stesso alla Funzione Finanza;
  - c) tipologie di transazioni eseguibili direttamente dalle varie funzioni aziendali;
  - d) controlli specifici e preventivi da applicarsi in casi, tassativamente previsti, in deroga alla normale procedura (es. pagamenti urgenti);
  - e) regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e discrezionalità;
  - f) controllo della correttezza dei flussi finanziari aziendali con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo;

- selezione e valutazione dei consulenti/agenti con previsione, fra l'altro, di quanto di seguito indicato:

- a) criteri oggettivi e trasparenti per la selezione (richiesta dei requisiti soggettivi relativi alla professionalità e all'onorabilità, iscrizione alle liste/albi di categoria, richiesta di documentazione quale certificato del casellario giudiziario/carichi pendenti, referenze qualificanti, ecc.);
- b) competitive bidding fra più consulenti;
- c) separazione di funzioni tra coloro che selezionano e coloro che ne controllano l'operato;
- d) modalità di gestione delle eccezioni alla procedura standard (ad esempio, acquisti di consulenze senza competitive bidding e/o in situazioni di emergenza);
- e) assunzione del personale con previsione, fra l'altro, di quanto di seguito indicato:
- f) criteri di selezione dei candidati oggettivi e trasparenti (ad esempio, voto di laurea/diploma, conoscenza di lingue straniere, precedenti esperienze professionali, ecc.);
- g) tracciabilità delle fonti di reperimento dei curricula (ad esempio, inserzioni, domande spontanee, segnalazioni interne, società di head-hunting, ecc.);
- h) modalità distinte di valutazione, "attitudinale" e "tecnica", del candidato, affidate a soggetti diversi che sottoscrivano le valutazioni medesime in modo da garantire la tracciabilità delle scelte effettuate;
- i) segregazione delle funzioni coinvolte nel processo di richiesta di assunzione di personale e in quello di valutazione/selezione o promozione del personale stesso;
- j) definizione di ruoli e responsabilità dei soggetti coinvolti; vi) modalità di archiviazione della documentazione rilevante;

- gestione degli omaggi e iniziative promozionali con previsione, fra l'altro, di quanto di seguito indicato:

- a) definizione di ruoli/responsabilità dei soggetti coinvolti;
- b) definizione delle categorie dei possibili beneficiari degli omaggi, iniziative promozionali e apparecchiature in comodato;
- c) indicazione di limiti di valore degli omaggi e delle apparecchiature concesse in comodato, nonché di limiti di durata dei contratti di comodato;
- d) definizione di importi massimi e specifiche autorizzazioni per le spese di viaggio di clienti e potenziali clienti;
- e) tracciabilità del processo decisionale e delle relative motivazioni;
- f) conservazione della documentazione rilevante.

#### Sistema deleghe, poteri di firma e poteri autorizzativi

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

#### Tracciabilità

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti. Lo scambio di comunicazioni, informazioni e autorizzazioni tra i soggetti coinvolti nei rispettivi processi è soggetto ad obblighi di conservazione in appositi e sicuri archivi non accessibili a terzi. Particolare attenzione deve essere prestata anche nel caso di utilizzo di sistemi informatici per lo scambio di informazioni (e-mail e documenti elettronici devono essere conservati in appositi spazi elettronici non accessibili a terzi e protetti da adeguati sistemi di password).

### **3.2.2 Controlli specifici**

#### Report

Devono esistere report periodici sull'utilizzo di risorse finanziarie con motivazioni e beneficiari, inviati ad adeguato livello gerarchico e archiviati.

#### Registrazione

L'operazione deve essere registrata e documentata come da procedure aziendali. Devono esistere documenti giustificativi delle risorse finanziarie utilizzate, con motivazione e attestazione di inerenza e congruità, approvati da adeguato livello gerarchico ed archiviati.

#### Sicurezza informatica

Deve essere affidata esclusivamente a una Funzione competente, che ne deve assicurare la tracciabilità la cancellazione di dati, liste di controllo e archivi.

Devono esistere liste di controllo degli accessi ai sistemi informativi e automatismi di segnalazione all'amministratore del sistema di operazioni non autorizzate: cancellazioni, tentativi di accesso, alterazione delle funzionalità del sistema.

#### Quadratura e Riscontri

Devono essere previste attività periodiche di quadratura dei dati e dei relativi riscontri.

#### Elenco dei beneficiari di omaggi/utilità

Deve essere redatto un elenco dei soggetti cui vengono inviati omaggi, con specifica indicazione dei soggetti riconducibili alla Pubblica Amministrazione e dell'omaggio destinato a ciascun beneficiario.

## 4. Abusi di mercato

La Parte Speciale denominata “Abusi di mercato” che si applica alle tipologie specifiche di reati specificati dall’art. 25-sexies del Decreto e di illeciti amministrativi specificati dall’art. 187-quinquies TUF (riconducibili al c.d. “abuso di mercato”), descrive e illustra regole di condotta e controlli che tutti i destinatari adottano ed applicano al fine di prevenire il verificarsi dei reati e gli illeciti amministrativi sopra specificati.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nella “Codice Etico” e nelle policy aziendali che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell’ente.

### 4.1 Analisi delle fattispecie di reato

E’ opportuno mettere in evidenza come, con riferimento all’abuso di mercato, l’ente non è responsabile se dimostra che le persone hanno agito esclusivamente nell’interesse proprio o di terzi.

Il regime sanzionatorio dell’ente per i reati di abuso di mercato è esclusivamente di natura pecuniaria, non essendo prevista, neanche in sede cautelare, l’irrogabilità delle sanzioni interdittive.

Le disposizioni si applicano, ai sensi dell’art. 182 TUF:

- anche agli abusi di mercato sono commessi all’estero, qualora attengano a strumenti finanziari ammessi o per i quali è stata fatta richiesta d’ammissione alla negoziazione in un mercato regolamentato italiano;
- per i fatti concernenti strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata una richiesta d’ammissione alla negoziazione in un mercato regolamentato italiano o di un altro Stato membro.

Le disposizioni in materia di abusi di mercato non si applicano alle negoziazioni di azioni, obbligazioni e altri strumenti finanziari propri quotati, effettuate nell’ambito di programmi di riacquisto da parte dell’emittente o di enti controllati o collegati, ed alle operazioni di stabilizzazione di strumenti finanziari che rispettino le condizioni stabilite dalla Consob con regolamento (art. 183 TUF).

Di seguito, si riporta una breve descrizione dei reati richiamati dall’art. 25-sexies (Abusi di mercato) del Decreto, introdotto dall’art. 9 della legge n. 62/2005.

E’ opportuno evidenziare che:

- qualora si tratti di delitti, tali fattispecie sono punibili anche a titolo di tentativo, ai sensi dell’art. 56 c.p.;
- un ulteriore ampliamento della punibilità è legato alla possibilità di concorrere consapevolmente con altri soggetti nella realizzazione delle fattispecie di reato (nell’ipotesi di concorso di più persone nella commissione di un reato, disciplinata dall’art. 110 c.p.), apportando quindi un contributo che può essere minore rispetto alla realizzazione integrale della fattispecie prevista dal legislatore.

#### Abuso di informazioni privilegiate (art. 184 TUF)

Commette il reato di abuso di informazioni privilegiate:

- 1) chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:
  - a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
  - b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
  - c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a);
- 2) chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al punto 1).

E' previsto un aggravamento della pena, con un aumento della multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

Il dolo consiste nella coscienza e volontà di utilizzare informazioni privilegiate compiendo operazioni su strumenti finanziari ovvero raccomandando o inducendo altri a compiere dette operazioni ovvero ancora comunicando le informazioni ad altri al di fuori dei propri ordinari compiti professionali.

Il reato si consuma all'atto dell'utilizzo di informazioni privilegiate, identificato nel compiere operazioni, direttamente o indirettamente, su strumenti finanziari, nel raccomandare o indurre altri al compimento di tali operazioni, nel comunicare le informazioni ad altri esorbitando dai propri ordinari compiti professionali;

#### Manipolazione del mercato (art. 185 TUF)

La condotta sanzionata consiste nella diffusione di notizie false o nel porre in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

E' previsto un aggravamento della pena, con un aumento della multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

Il dolo consiste nella coscienza e volontà di diffondere notizie false o di porre in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

Il reato si consuma all'atto della diffusione di notizie false e della effettuazione di operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

#### Illeciti amministrativi di abuso di mercato

Riportiamo, qui di seguito, una breve descrizione degli illeciti amministrativi di abuso di mercato, specificati dall'art. 187-quinquies TUF, ai quali è riconducibile la responsabilità amministrativa dell'ente.

#### Abuso di informazione privilegiate (art. 187-bis TUF)

Salve le sanzioni penali quando il fatto costituisce reato, commette illecito amministrativo chiunque:

- 1) essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:
  - a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
  - b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
  - c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a);
- 2) essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al punto 1);
- 3) essendo in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse, compie taluno dei fatti descritti al punto 1).

Le sanzioni amministrative pecuniarie previste sono aumentate fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dall'illecito quando, per le qualità personali del colpevole ovvero per l'entità del prodotto o del profitto conseguito dall'illecito, esse appaiono inadeguate anche se applicate nel massimo.

La condotta prevista nell'articolo in commento ricalca sostanzialmente quella già contemplata dall'illecito penale. A differenza di quest'ultimo, si considera nell'area di punibilità anche l'illecito commesso da chi che, anche incidentalmente, venga in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse (c.d. insider secondario).

Per le fattispecie previste dal presente articolo il tentativo è equiparato alla consumazione.

#### Manipolazione del mercato (art. 187-ter TUF)

Salve le sanzioni penali quando il fatto costituisce reato, commette illecito amministrativo:

- 1) chiunque, tramite mezzi di informazione, compreso internet o ogni altro mezzo, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari. Per i giornalisti che operano nello svolgimento della loro attività professionale la diffusione delle informazioni va valutata tenendo conto delle norme di autoregolamentazione proprie di detta professione, salvo che tali soggetti traggano, direttamente o indirettamente, un vantaggio o un profitto dalla diffusione delle informazioni;
- 2) chiunque pone in essere:
  - a) operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
  - b) operazioni od ordini di compravendita che consentono, tramite l'azione di una o di più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;
  - c) operazioni od ordini di compravendita che utilizzano artifici od ogni altro tipo di inganno o di espediente;

- d) altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

Per gli illeciti indicati al punto 2, lettere a) e b), non può essere assoggettato a sanzione amministrativa chi dimostri di avere agito per motivi legittimi e in conformità alle prassi di mercato ammesse nel mercato interessato.

Le sanzioni amministrative pecuniarie previste dai commi precedenti sono aumentate fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dall'illecito quando, per le qualità personali del colpevole, per l'entità del prodotto o del profitto conseguito dall'illecito ovvero per gli effetti prodotti sul mercato, esse appaiono inadeguate anche se applicate nel massimo.

#### **4.2 Attività sensibili**

Le principali attività sensibili in relazione agli abusi di mercato che l'ente ha individuato al proprio interno sono le seguenti:

##### **Gestione delle informazioni privilegiate**

Si tratta della gestione delle "informazioni privilegiate" ai sensi dell'articolo 181 TUF acquisite nell'ambito dell'attività di distribuzione di prodotti finanziari.

##### **Gestione delle comunicazioni verso l'esterno**

Si tratta della gestione delle attività di diffusione di notizie circa le strategie aziendali (industriali e finanziarie) dell'ente o dell'ente controllante o di quelle controllate, ovvero diffusione di notizie attraverso le relazioni semestrali o la relazione e redazione del bilancio di esercizio ovvero in merito alle stesse.

##### **Gestione dell'attività di negoziazione di strumenti finanziari**

Si tratta dell'attività relative alla gestione del portafoglio titoli, operazioni sul capitale e operazioni di compravendita di azioni o quote dell'ente o dell'ente controllante o di quelle controllate, contatti o rapporti, anche per via mediata, con soci di maggioranza o con altri enti i cui titoli siano negoziabili su mercati finanziari regolamentati.

#### **4.3 Sistema dei controlli**

Il sistema dei controlli applicabili alle attività sensibili individuate è stato definito utilizzando, come riferimento, le Linee Guida ad oggi pubblicate dalle principali associazioni di categoria nonché le best practice internazionali in tema di abusi di mercato.

Pertanto, già il corretto e continuativo adempimento delle suddette disposizioni potrebbe essere importante e sufficiente strumento di salvaguardia, specie ove si aumenti l'attenzione mediante verifiche e controlli specifici.

In ogni caso, sono, di seguito, individuati gli standard di controllo specificatamente individuati per aree di attività dell'ente che includono le attività sensibili come sopra indicate.

Il Modello contempla l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili.

##### **4.3.1 Controlli generali**

I controlli generali individuati sono i seguenti:

Separazione delle responsabilità / funzioni / processo

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

Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

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

Sistema deleghe, poteri di firma e poteri autorizzativi

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività di individuazione dei nominativi che hanno accesso alle informazioni, la valutazione delle informazioni privilegiate, l'identificazione di eventuali disclosure e/o limitazioni operative per i nominativi iscritti nel Registro e l'istituzione e la gestione del Registro.

Tracciabilità

Devono esistere presidi che, in relazione ad ogni comunicazione scritta relativa a ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti. Lo scambio di comunicazioni, informazioni e autorizzazioni tra i soggetti coinvolti nei rispettivi processi è soggetto ad obblighi di conservazione in appositi e sicuri archivi non accessibili a terzi. Particolare attenzione deve essere prestata anche nel caso di utilizzo di sistemi informatici per lo scambio di informazioni (e-mail e documenti elettronici devono essere conservati in appositi spazi elettronici non accessibili a terzi e protetti da adeguati sistemi di password).

#### **4.3.2 Controlli specifici**

Qui di seguito si evidenziano, i controlli specifici per le aree di attività dell'ente che includono le attività sensibili sopra individuate che si aggiungono al rigoroso rispetto del "Codice Etico" e delle policy aziendali. L'elencazione individua uno standard minimo di comportamento in dette attività e fa salve le eventuali procedure di controllo di maggiore tutela o più specifiche per lo svolgimento di attività connesse alle attività sensibili.

**Gestione delle informazioni privilegiate**

Relativamente alla gestione delle informazioni che si possono definire privilegiate ai sensi dell'articolo 181 TUF, gli standard di controllo specifici sono i seguenti:

Obbligo di segnalazione

Lo standard prevede l'obbligo di segnalazione dell'accesso a informazioni privilegiate.

Autorizzazione formale

Deve esistere un'autorizzazione formalizzata alla diffusione di informazioni privilegiate.

Vincoli di confidenzialità

Devono esistere vincoli formalizzati (normative aziendali e comunicazioni, clausole contrattuali) per l'adozione di misure di confidenzialità volte a garantire la sicurezza organizzativa, fisica e logica e la riservatezza delle informazioni privilegiate/rilevanti di cui dipendenti / consulenti esterni vengano a conoscenza.

Registrazione

Deve esistere un registro delle persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, hanno accesso alle informazioni privilegiate.

Attività di formazione

Devono essere svolte attività di formazione di base sul tema del riconoscimento e del trattamento delle informazioni privilegiate e sulla normativa vigente in materia, rivolte al personale che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, può avere accesso alle informazioni privilegiate e attività di formazione rivolta al personale coinvolto nel processo di gestione delle informazioni privilegiate.

#### Sicurezza informatica

Lo standard impone la necessaria esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel d. lgs. n. 196/03 e nelle best practice internazionali.

#### **Gestione delle comunicazioni verso l'esterno**

Con riferimento a tale attività sensibile, gli standard di controllo specifici sono i seguenti:

##### Obbligo di segnalazione

Deve essere segnalata la volontà di comunicare notizie o dati verso all'esterno al diretto superiore gerarchico.

##### Autorizzazioni formalizzate

Devono esistere autorizzazioni formalizzate per l'esecuzione di un'attività di comunicazione verso l'esterno.

##### Vincoli di confidenzialità

Lo standard richiede che debbano esistere vincoli formalizzati (procedure o circolari interne, clausole contrattuali) per il mantenimento della confidenzialità delle informazioni rilevanti di cui dipendenti/consulenti esterni vengano a conoscenza. Tali vincoli devono espressamente prevedere il divieto di diffusione dell'informazione rilevante all'interno o all'esterno dell'ente, se non tramite il canale istituzionalmente previsto.

##### Attività di formazione

Devono essere svolte attività di formazione di base, rivolte al personale coinvolto nel processo di comunicazione verso l'esterno, e attività di formazione rivolta agli amministratori, al management e ai dipendenti delle aree/funzioni aziendali sensibili sulla normativa in materia di abusi di mercato. che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, può avere accesso alle informazioni privilegiate e attività di formazione rivolta al personale coinvolto nel processo di comunicazione verso l'esterno.

#### Sicurezza informatica

Lo standard impone la necessaria esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel d. lgs. n.196/03 e nelle best practice internazionali.

#### **Gestione dell'attività di negoziazione di strumenti finanziari.**

Relativamente a tale attività sensibile, gli standard di controllo specifici sono i seguenti:

##### Autorizzazione formale

Deve esistere un'autorizzazione formalizzata all'esecuzione di operazioni su strumenti finanziari.

##### Vincoli di confidenzialità

Devono esistere vincoli formalizzati (normative aziendali e comunicazioni, clausole contrattuali) per l'adozione di misure di confidenzialità volte a garantire la riservatezza delle operazioni.

##### Report

Devono esistere report periodici rivolti alle funzioni/organi preposti contenenti le informazioni relative alle operazioni su strumenti finanziari eseguite e su quelle ordinate ma non eseguite.

Registrazione

L'operazione avente ad oggetto strumenti finanziari deve essere registrata e documentata come da procedure aziendali.

Quadratura e Riscontri

Devono essere previste attività periodiche di quadratura dei dati e dei relativi riscontri.

Attività di formazione

Devono essere svolte attività di formazione sul tema della gestione delle operazioni su strumenti finanziari e sulla normativa vigente in materia, rivolte al personale che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, è coinvolto nell'attività sensibile in oggetto.

Sicurezza informatica

Lo standard impone la necessaria esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel d. lgs. 196/03 e nelle best practice internazionali.

## 5. Reati con finalità di terrorismo o di eversione dell'ordine democratico

La presente Parte Speciale descrive e illustra regole di condotta e controlli che tutti i Destinatari adottano ed applicano al fine di prevenire il verificarsi dei reati previsti dall'art. 25-quater del Decreto.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### 5.1 Analisi delle fattispecie di reato

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del Decreto, riportiamo qui di seguito una descrizione, in forma sintetica, dei contenuti dell'articolo 25-quater (Delitti con finalità di terrorismo o di eversione dell'ordine democratico) introdotto nel Decreto dall'art. 3 della legge 14 gennaio 2003, n. 7 e dei reati cui tale articolo fa riferimento.

L'articolo in esame prevede l'applicazione di sanzioni all'ente i cui soggetti apicali o i sottoposti alla direzione o alla vigilanza dei citati apicali compiano delitti aventi finalità di terrorismo o di eversione dell'ordine democratico qualora l'ente – o una sua unità organizzativa – venga usata allo scopo di consentire o agevolare la commissione di tali reati.

Si tratta, in particolare, dei "delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali" (art. 25-quater, comma 1, d. lgs. n. 231/2001), nonché dei delitti, diversi da quelli sopra indicati, "che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999" (art. 25-quater, comma 4, d. lgs. n. 231/2001).

La genericità dei richiami operati dall'art. 25-quater del Decreto crea non pochi problemi con riferimento all'esatta individuazione delle fattispecie delittuose che possono comportare l'applicazione della disciplina prevista dal citato Decreto.

Quanto alla categoria dei "delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali", si possono individuare quali principali reati presupposto della responsabilità ex Decreto:

#### Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

L'articolo 270- bis c.p. il quale punisce chi promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti violenti con finalità terroristiche od eversive.

#### Assistenza agli associati

L'articolo 270- ter c.p. il quale punisce chi dà rifugio o fornisce vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni con finalità terroristiche od eversive .

Per quanto, invece, concerne i reati di cui alla Convenzione di New York, si rileva che quest'ultima punisce chiunque, illegalmente e dolosamente, fornisce o raccoglie fondi sapendo che gli stessi saranno, anche parzialmente, utilizzati per compiere:

- atti diretti a causare la morte o gravi lesioni di civili, quando con ciò si realizzi un'azione finalizzata ad intimidire una popolazione, o coartare un governo o un'organizzazione internazionale;

- atti costituenti reato ai sensi delle Convenzioni in materia di: sicurezza del volo e della navigazione; tutela del materiale nucleare; protezione di agenti diplomatici; repressione di attentati mediante uso di esplosivi.

La punibilità sussiste per tutti i complici ed anche qualora i fondi non vengano poi effettivamente usati per il compimento dei reati sopra descritti.

## 5.2. Attività sensibili

L'analisi dei processi aziendali ha consentito di individuare quale attività sensibile, con riferimento ai reati previsti dall'art. 25-quater del Decreto, quella relativa a gestione degli adempimenti antiterrorismo.

- **Adempimenti antiterrorismo**
- **Gestione di iniziative umanitarie e di solidarietà in favore di enti con sede o operanti in paesi considerati a rischio**

In particolare:

- attività legate all'esecuzione delle istruzioni, e conseguenti procedure interne, in materia di antiriciclaggio (incluso il sistema di monitoraggio che consenta all'ufficio preposto di effettuare tempestivamente le opportune segnalazioni), in tutti i casi di rapporto con la clientela, per favorirne la conoscenza, delle modalità delle eventuali operazioni sottostanti la richiesta di garanzie o fidejussioni, delle motivazioni che inducono o hanno indotto a tale richiesta;
- attività di investimento con il patrimonio libero;
- attività di vendita o locazione di immobili e singole operazioni a livello transnazionale, di prodotti a contenuto finanziario.

## 5.3 Sistema dei controlli interni

Il sistema dei controlli applicabili all'attività individuata è stato definito sulla base delle indicazioni fornite dalle Linee Guida pubblicate dalle principali associazioni di categoria nonché dalle best practice internazionali in tema di repressione del finanziamento del terrorismo.

Per ognuna delle attività, oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, sono stati individuati i seguenti standard di controllo.

Il Modello prevede l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili;
- Controlli relativi alle attività sensibili sopra individuate siano, in tutto o in parte, affidate a soggetti esterni all'ente.

### 5.3.1 Controlli generali

I controlli generali sono i seguenti:

#### Separazione delle responsabilità/funzioni/processo

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

#### Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Devono esistere disposizioni aziendali idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività.

#### Sistema deleghe, poteri di firma e poteri autorizzativi

Devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi.

#### Tracciabilità

Deve essere assicurata la tracciabilità della documentazione e delle relative fonti e degli elementi informativi, nonché la relativa archiviazione.

Deve essere garantita la tracciabilità del sistema informatico utilizzato per la trasmissione di dati e informazioni dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema.

### **5.3.2 Controlli specifici**

Qui di seguito si individuano, i controlli specificatamente individuati per le aree di attività dell'ente che includono l'attività sensibile della gestione degli adempimenti antiterrorismo.

Gli standard di controllo specifici per le attività sensibili sopra individuate sono i seguenti:

#### Verifiche preventive

Devono essere diffuse, al personale coinvolto nell'attività tipica aziendale, liste nominative, stilate da organismi ufficiali (es. liste approvate dall'Unione europea per l'applicazione delle misure di congelamento e di divieto di prestazione dei servizi finanziari, diffuse dall'UIF), che permettano di effettuare gli opportuni controlli prima di procedere alla stipulazione di un contratto.

#### Pagamento dei corrispettivi contrattuali

Con riferimento alla fase di pagamento dei corrispettivi contrattualmente previsti deve esistere una procedura che preveda che:

- il pagamento non possa essere effettuato in contanti o con strumenti di pagamento analoghi, in accordo con la normativa vigente;
- il pagamento relativo a beni o servizi acquistati dall'ente debba essere effettuato esclusivamente sul conto corrente indicato nei documenti contrattuali, salvo il caso di cessione del credito autorizzata dall'ente;
- i pagamenti non possano, in nessun caso, essere effettuati su conti correnti cifrati;
- il pagamento effettuato su conti correnti di banche appartenenti od operanti in paesi elencati tra i così detti "paradisi fiscali", o in favore di enti off shore, sia autorizzato da un adeguato livello gerarchico;
- il pagamento corrisponda esattamente a quanto indicato nel contratto;
- il pagamento relativo a beni o servizi acquistati dall'ente non possa essere effettuato in favore di un soggetto diverso dalla controparte contrattuale (con verifica di coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione);
- il pagamento relativo a beni o servizi acquistati dall'ente non possa essere effettuato in un paese terzo rispetto a quello delle parti contraenti o a quello di esecuzione del contratto;

- vi siano idonei sistemi di monitoraggio al fine di evitare pagamenti in favore di soggetti rientranti nelle black list stilate da organismi ufficiali, anche esteri;
- sia assicurata la tracciabilità del pagamento (importo, nome/denominazione, indirizzo e numero di conto corrente).

Monitoraggio

Devono esistere idonei sistemi di monitoraggio che consentano all'ufficio preposto di effettuare tempestivamente le opportune segnalazioni all'UIF.

**5.3.3 Controlli relativi ad attività sensibili affidate, in tutto o in parte, a soggetti esterni all'ente**

Nel caso in cui una delle sopra elencate attività sensibili sia, in tutto o in parte, affidata, in virtù di appositi accordi, a soggetti esterni all'ente, anche appartenenti al medesimo gruppo, il sistema di controllo adottato concerne la previsione, negli accordi e/o nei documenti che disciplinano lo svolgimento di tali attività la previsione di specifiche clausole:

- con cui il terzo dichiara l'impegno a dotarsi di misure idonee a prevenire il rischio di commissione dei reati richiamati dal d. lgs. n. 231/2001, nello svolgimento delle attività per conto dell'ente, che potrebbero essere ascritti all'ente;
- che attribuiscono, quando ritenuto opportuno, all'ente la possibilità di effettuare degli audit per verificarne il rispetto;
- che disciplinino le conseguenze della violazione da parte del terzo delle norme di cui al d. lgs. n. 231/2001 (es. clausola risolutiva espressa, penali) e degli standard concordati nei documenti contrattuali.

## **6. Reati di ricettazione, riciclaggio e impiego di denaro, di beni o di utilità di provenienza illecita**

La presente Parte Speciale descrive e illustra regole di condotta e controlli che tutti i Destinatari adottano ed applicano al fine di prevenire il verificarsi dei reati previsti dall'art. 25-octies del Decreto.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### **6.1 Analisi delle fattispecie di reato**

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del Decreto, si citano qui di seguito i reati, individuati dall'art. 25-octies del Decreto (introdotto dall'art. 63, comma 3, del d. lgs. n. 231/2007), alla cui commissione da parte di soggetti riconducibili all'ente (soggetti apicali e persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali, ai sensi dell'art. 5 del Decreto) è collegato il regime di responsabilità a carico dell'ente.

L'ente è ora punibile per i reati in esame anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un interesse o vantaggio per la società medesima, dopo l'abrogazione dei commi 5 e 6 dell'art. 10 della legge n. 146/2006 che prevedevano a carico della società la responsabilità e le sanzioni ex d. lgs. n. 231/2001 per i reati di riciclaggio e impiego di denaro, beni o utilità di provenienza illecita caratterizzati dall'elemento della trans nazionalità:

#### *Ricettazione (art. 648 c.p.)*

L'art. 648 c.p. incrimina chi "fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare".

Per acquisto si intende l'effetto di un attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.

Il termine ricevere sta ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.

Per occultamento si intende il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto.

La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione tra l'autore del reato principale e il terzo acquirente.

L'ultimo comma dell'art. 648 c.p. estende la punibilità "anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto".

#### *Riciclaggio (art. 648-bis c.p.)*

Tale reato consiste nel fatto di chiunque "fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa".

Il delitto in esame sussiste quando, antecedentemente ad esso, sia stato commesso un delitto non colposo al quale, però, il riciclatore non abbia partecipato a titolo di concorso.

La disposizione è applicabile anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto. E' rilevante il fatto di chi ponga ostacoli alla identificazione dei beni suddetti dopo che essi sono stati sostituiti o trasferiti.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).

È il reato commesso da "chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 (Ricettazione) c.p. e 648-bis (Riciclaggio) c.p., impiega in attività economiche o finanziarie denaro o beni o altre utilità provenienti da delitto".

Il riferimento specifico al termine "impiegare", di accezione più ampia rispetto a "investire" che suppone un impiego finalizzato a particolari obiettivi, esprime il significato di "usare comunque". Il richiamo al concetto di "attività" per indicare il settore di investimento (economia o finanza) consente viceversa di escludere gli impieghi di denaro od altre utilità che abbiano carattere occasionale o sporadico.

La specificità del reato rispetto a quello di riciclaggio risiede nella finalità di far perdere le tracce della provenienza illecita di denaro, beni o altre utilità, perseguita mediante l'impiego di dette risorse in attività economiche o finanziarie.

Sono, quindi, punite quelle attività che, a differenza del riciclaggio, non sostituiscono immediatamente i beni provenienti da delitto, ma che comunque contribuiscono alla "ripulitura" dei capitali illeciti.

## **6.2 Attività sensibili**

L'analisi dei processi aziendali dell'ente ha consentito di individuare quali attività sensibili che presentano il rischio di commissione dei reati previsti dall'art. 25-octies del Decreto:

**Attività di vendita di prodotti finanziari e di altri servizi di investimento**

**Rapporti con controparti per l'acquisto di beni e/o servizi di importo rilevante e gli investimenti**

## **6.3 Sistema dei controlli identificati in relazione alle attività sensibili individuate**

Il sistema dei controlli applicabili all'attività individuata è stato definito sulla base delle indicazioni fornite dalle Linee Guida pubblicate dalle principali associazioni di categoria nonché dalle best practice internazionali in tema di repressione del riciclaggio di denaro.

Per ognuna delle attività, oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, sono stati individuati standard di controllo. In particolare, Il Modello prevede l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili;
- Controlli relativi alle attività sensibili sopra individuate siano, in tutto o in parte, affidate a soggetti esterni all'ente.

### **6.3.1 Controlli generali**

I controlli generali sono i seguenti:

Separazione delle responsabilità/funzioni/processo

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

Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Devono esistere disposizioni aziendali idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività.

Sistema deleghe, poteri di firma e poteri autorizzativi

Devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi.

Tracciabilità

Deve essere assicurata la tracciabilità della documentazione e delle relative fonti e degli elementi informativi, nonché la relativa archiviazione.

Deve essere garantita la tracciabilità del sistema informatico utilizzato per la trasmissione di dati e informazioni dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema.

### **6.3.2 Controlli specifici**

Gli standard di controllo specifici per le attività sensibili individuate sono i seguenti:

**Attività di vendita di prodotti finanziari e di altri servizi di investimento**

Oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

Verifiche preventive, monitoraggio e segnalazioni

Devono essere predisposti e utilizzati adeguati presidi, strumenti organizzativi e procedure di riscontro per il corretto svolgimento dei controlli finalizzati, ai sensi della normativa vigente, al rispetto del principio fondamentale della "adeguata verifica" della clientela e dei correlati obblighi di segnalazione. Tra questi rientrano tutti gli adempimenti previsti dalla normativa specifica (i c.d. presidi antiriciclaggio), tra i quali, in particolare, la corretta gestione dell'archivio unico informatico (AUI) e di un sistema informatico di ausilio alla gestione delle attività rivolte alla prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose.

Report

Deve essere prevista, con cadenza periodica stabilita, la predisposizione, da parte della funzione competente, di report che - inviati a adeguato livello gerarchico – permettano verifiche sullo stato della gestione del sistema antiriciclaggio, sull'attività svolta in ambito antiriciclaggio, sul rispetto della normativa e sullo stato di implementazione e gestione degli applicativi rispetto ai requisiti imposti dalla normativa vigente e dalle eventuali policy aziendali;

Formazione

Devono essere predisposti adeguati programmi di formazione del personale ritenuto esposto al rischio riciclaggio;

Verifica sul pagamento dei corrispettivi contrattuali

Per il contenuto del quale si rinvia a quanto previsto in merito a tali controlli nella Parte Speciale sui "Reati con finalità di terrorismo o di eversione dell'ordine democratico" con particolare attenzione alla verifica della regolarità dei pagamenti anche con riferimento alla coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione.

**Rapporti con controparti per l'acquisto di beni e/o servizi di importo rilevante e gli investimenti.**

Oltre al rigoroso rispetto del documento denominato “Codice Etico” e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

Verifica dell’attendibilità commerciale e professionale dei fornitori, partner commerciali e, in generale, delle controparti

Deve essere svolta, con particolare riferimento ai fornitori di beni e servizi di importo rilevante e delle controparti in relazione ad attività di investimento, una verifica sulla base di alcuni indici predefiniti (ad es. dati pregiudizievoli pubblici - protesti, procedure concorsuali - o acquisizione di informazioni commerciali tramite società specializzate verifica dell’idoneità della struttura aziendale a fornire i beni/servizi necessari; entità del prezzo sproporzionata rispetto ai valori medi di mercato);

Selezione fornitori

Deve svolgersi un controllo sul rispetto delle procedure interne per la valutazione degli offerenti e delle offerte e accertare che sia possibile ricostruire la filiera decisionale;

Verifica sul pagamento dei corrispettivi contrattuali

Per il contenuto del quale si rinvia a quanto previsto in merito a tali controlli nella Parte Speciale “Reati con finalità di terrorismo o di eversione dell’ordine democratico” con particolare attenzione alla verifica della regolarità dei pagamenti anche con riferimento alla coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione.

**6.3.3 Controlli relativi ad attività sensibili affidate, in tutto o in parte, a soggetti esterni all’ente**

Nel caso in cui una delle sopra elencate attività sensibili sia, in tutto o in parte, affidata, in virtù di appositi accordi, a soggetti esterni all’ente, il sistema di controllo adottato concerne la previsione, negli accordi e/o nei documenti che disciplinano lo svolgimento di tali attività la previsione di specifiche clausole:

- con cui il terzo dichiara l’impegno a dotarsi di misure idonee a prevenire il rischio di commissione dei reati richiamati dal d. lgs. n. 231/2001, nello svolgimento delle attività per conto dell’ente, che potrebbero essere ascritti all’ente;
- che attribuiscono, quando ritenuto opportuno, all’ente la possibilità di effettuare degli audit per verificarne il rispetto;
- che disciplinino le conseguenze della violazione da parte del terzo delle norme di cui al d. lgs. n. 231/2001 (es. clausola risolutiva espressa, penali) e degli standard concordati nei documenti contrattuali.

## 7. Delitti contro la personalità individuale

La presente Parte Speciale descrive e illustra regole di condotta e controlli che tutti i Destinatari adottano ed applicano al fine di prevenire il verificarsi dei delitti previsti dall'art. 25-quinquies del Decreto.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nella "Codice Etico" e nelle policy aziendali specifiche che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### 7.1 Analisi delle fattispecie di reato

Di seguito, si riportano i contenuti dell'articolo 25-quinquies (Delitti contro la personalità individuale), introdotto nel Decreto dall'art. 5 della legge 11 agosto 2003, n. 228 (Ratifica della Convenzione internazionale contro il finanziamento del terrorismo) e modificato e integrato dalla legge 6 febbraio 2006, n. 38, che prevede la sanzionabilità amministrativa dell'ente in relazione ai seguenti delitti:

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

### 7.2 Attività sensibili

L'analisi dei processi aziendali dell'ente ha consentito di individuare le seguenti attività sensibili che presentino il rischio di commissione dei reati previsti dall'articolo 25-quinquies del Decreto.

Più precisamente, si tratta delle attività di:

#### **Promozione e/o gestione di iniziative umanitarie e di solidarietà**

Gestione dell'organizzazione delle "attività sociali"

#### **Gestione siti internet e intranet**

Si tratta della gestione delle attività delle unità che propongono le modifiche, l'introduzione di nuove informazioni sul sito Intranet/Internet o l'attivazione dell'accesso alla rete ad un dipendente, le unità che le autorizzano, le unità che gestiscono l'inserimento dei dati sul sistema e le unità che verificano il corretto inserimento dei dati.

#### **Organizzazione e promozione di viaggi (viaggi premio) per dipendenti o partner commerciali**

Si tratta dell'attività di organizzazione e promozione di viaggi premio per dipendenti, collaboratori e partner commerciali.

**Attività che coinvolgono direttamente minori, soprattutto per finalità didattiche, sportive o ricreative**

Gestione dell'organizzazione delle "attività sociali" che coinvolgono minorenni.

### **7.3 Sistema dei controlli**

Il sistema dei controlli applicabili alle attività individuate è stato definito sulla base delle indicazioni fornite dalle Linee Guida pubblicate dalle principali associazioni di categoria nonché dalle best practice internazionali in tema di repressione del finanziamento del terrorismo.

Per ognuna delle attività, oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, sono stati individuati i seguenti standard di controllo.

Il Modello prevede l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili.

#### **7.3.1 Controlli generali**

I controlli generali (ovvero valevoli per tutte le attività sensibili individuate) sono i seguenti:

**Separazione delle responsabilità/funzioni/processo**

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

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

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

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

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

**Tracciabilità**

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti. Lo scambio di comunicazioni, informazioni e autorizzazioni tra i soggetti coinvolti nei rispettivi processi è soggetto ad obblighi di conservazione in appositi e sicuri archivi non accessibili a terzi. Particolare attenzione deve essere prestata anche nel caso di utilizzo di sistemi informatici per lo scambio di informazioni (e-mail e documenti elettronici devono essere conservati in appositi spazi elettronici non accessibili a terzi e protetti da adeguati sistemi di password).

#### **7.3.2 Controlli specifici**

Di seguito si individuano degli standard minimi di controllo specificatamente individuati per aree di attività dell'ente che includono le attività sensibili sopra individuate:

**Promozione e/o gestione di iniziative umanitarie e di solidarietà**

Oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

#### Autorizzazione

La promozione e/o gestione di iniziative umanitarie e di solidarietà deve essere adeguatamente autorizzate, formalizzate e rendicontate.

#### Codice Etico

Il Codice Etico deve prevedere principi relativi alla promozione e/o gestione di iniziative umanitarie e di solidarietà

#### **Gestione siti internet e intranet**

Oltre al rigoroso rispetto del documento denominato “Codice Etico” e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

#### Autorizzazione

La pubblicazione di informazioni sui siti internet ed intranet deve essere adeguatamente autorizzata, formalizzata e rendicontata.

#### Codice Etico

Il Codice Etico deve prevedere il divieto di acquisire, utilizzare, diffondere e/o cedere materiale pedo-pornografico.

#### **Organizzazione e promozione di viaggi (viaggi premio) per dipendenti o partner commerciali.**

Oltre al rigoroso rispetto del documento denominato “Codice Etico” e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

#### Autorizzazione

L'organizzazione e la promozione di viaggi premio devono essere adeguatamente autorizzate, formalizzate e rendicontate.

#### Codice Etico

Il Codice Etico deve prevedere il divieto di acquisire, utilizzare, diffondere e/o cedere materiale pedo-pornografico.

#### **Attività che coinvolgono direttamente minori, soprattutto per finalità didattiche, sportive o ricreative**

Oltre al rigoroso rispetto del documento denominato “Codice Etico” e delle policy aziendali, gli standard di controllo specifici sono i seguenti:

#### Autorizzazione

L'organizzazione e la promozione di viaggi premio devono essere adeguatamente autorizzate, formalizzate e rendicontate.

#### Codice Etico

Il Codice Etico deve prevedere il divieto di finanziare attività che coinvolgono direttamente minori, soprattutto per finalità didattiche, sportive o ricreative in paesi noti per il non rispetto dei diritti umani.

## 8. Sicurezza sul lavoro

Nella Parte Speciale vengono illustrate le regole di condotta, le modalità di gestione dei processi ed i controlli adottati per l'adeguamento alla norme in tema di salute sul lavoro, al fine di prevenire il verificarsi dei reati previsti dall'art. 25-septies del Decreto.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### 8.1 Analisi delle fattispecie di reato

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del Decreto, riportiamo qui di seguito una descrizione sintetica dei reati previsti dall'articolo 25-septies (omicidio colposo e lesioni colpose gravi e gravissime, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro) introdotto dall'art. 9 della Legge 3 Agosto 2007, n. 123.

La norma statuisce la responsabilità dell'ente in relazione ai delitti di cui agli artt. 589 e 590, comma 3 del codice penale, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. L'accertamento della responsabilità dell'ente può determinare l'applicazione di una sanzione pecuniaria in misura non inferiore a mille quote e di sanzioni interdittive per una durata non inferiore a tre mesi e non superiore ad un anno.

Si tratta, in particolare, dei delitti di omicidio colposo e di lesioni colpose gravi e gravissime.

L'omicidio colposo consiste nella condotta di chi cagiona per colpa la morte di una persona: non c'è volontà di causare l'evento lesivo, ma esso si verifica per inosservanza delle norme poste a tutela della salute sul lavoro (colpa specifica).

La lesione colposa è il reato commesso da chi cagiona ad altri per colpa una lesione personale, vale a dire qualsiasi comportamento idoneo a determinare l'evento della malattia.

La lesione è grave se dal fatto deriva una malattia che mette in pericolo la vita della persona offesa o una malattia o incapacità ad attendere alle ordinarie occupazioni per più di 40 giorni; oppure se il fatto produce l'indebolimento permanente di un senso o organo.

La lesione è gravissima se dal fatto deriva malattia insanabile; perdita di un senso o di un arto o deformazione permanente del viso.

Considerando che la responsabilità dell'ente deriva dalla commissione dei reati sopra indicati solo qualora gli stessi fossero commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, è necessario determinare quali siano tali disposizioni. Dall'analisi normativa svolta, le principali disposizioni di legge in vigore in materia risultano essere le seguenti:

- D.P.R. 547 /55 per la prevenzione degli infortuni sul lavoro;
- D.P.R. 164 /56 per la prevenzione degli infortuni nelle costruzioni;
- D.P.R. 303 /56 per l'igiene del lavoro;
- Legge 186/68 per materiali, apparecchiature, impianti elettrici ed elettronici;
- D.P.R. 175/88 per le attività che presentano rischi di incidenti rilevanti;
- Legge 46/90 per la sicurezza degli impianti;
- D. Lgs. 277/91 per i rischi da esposizione ad agenti chimici, fisici e biologici;

- D. Lgs. 475/92 per i dispositivi di protezione individuale;
- D.P.R. 246/93 per i prodotto da costruzione;
- D. Lgs. 81/08 di riordino dell'intero settore;
- D. Lgs. 230/95 per la sicurezza in presenza di radiazioni ionizzanti;
- D.P.R. 459/96 per la sicurezza delle macchine;
- D. Lgs. 493/96 per la segnaletica;
- D. Lgs. 494/96 per la sicurezza nei cantieri;
- D.M. 10 Marzo 1998 per la sicurezza antincendio;
- D. Lgs. 151/01 per la tutela delle lavoratrici gestanti;
- D.M. 288/03 per il pronto soccorso;
- D. Lgs. 187/05 per i rischi derivanti dall'esposizione a vibrazioni meccaniche;
- D.M. 22 Febbraio 2006 per la progettazione, costruzione ed esercizio di edifici o locali destinati ad uffici;
- D. Lgs. 195/06 per i rischi da esposizione al rumore;
- D. Lgs. 257/06 per i rischi da esposizione all'amianto;
- Legge 123/07 per le misure in tema di tutela della salute e della sicurezza sul lavoro.

## **8.2 Attività sensibili**

L'analisi dei processi aziendali ha consentito di individuare quale attività sensibile, con riferimento ai reati previsti dall'articolo 25-septies del Decreto, quella relativa alla gestione degli adempimenti in materia di sicurezza sul lavoro.

L'attività sensibile individuata è:

### **Sicurezza e igiene sul lavoro (D.Lgs. 81/08 e successive modificazioni / integrazioni)**

Si tratta, in particolare, delle attività che la legislazione a tutela delle norme antinfortunistica, di tutela dell'igiene e della salute sul lavoro ha reso nel tempo obbligatorie, quali ad esempio:

- nomina di un Delegato alla sicurezza e salute;
- nomina di un Responsabile del Servizio di Prevenzione e Protezione (RSPP);
- creazione e gestione di un Sistema di Prevenzione e Protezione (SPP);
- nomina di preposti Addetti alla Prevenzione e Protezione (APP) e gestione dei rapporti con gli stessi;
- gestione dei rapporti con i Rappresentanti dei Lavoratori per la Sicurezza (RLS);
- impostazioni sulla Sorveglianza Sanitaria, con nomina di un medico responsabile;
- adozione di tutte le misure necessarie per rispettare la normativa in materia.

Altra area sensibile interessata dalla prevenzione della commissione dei reati 231 suindicati è rappresentata dall'affidamento di lavori ad imprese appaltatrici o a lavoratori autonomi, in considerazione del rafforzamento degli obblighi di sicurezza in capo al committente in caso di

stipula di contratti di appalto o contratto d'opera. Il datore di lavoro committente, ai sensi dell'art. 7 del D.Lgs. 81/08 (così come modificato dalla Legge 123/07) deve:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici e dei lavoratori autonomi;
- fornire dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sarà effettuato il lavoro e sulle misure di prevenzione di emergenza adottate;
- promuovere la redazione di un documento unico di valutazione dei rischi che indichi le misure adottate per eliminare le interferenze, da allegare al contratto;
- indicare specificamente i costi relativi alla sicurezza nei contratti di somministrazione, appalto e subappalto.

Inoltre con riferimento ai reati in materia di salute e sicurezza dai quali può scaturire la responsabilità amministrativa dell'ente, il d. lgs. n. 81 del 9 aprile 2008 recante il Testo Unico in materia di salute e sicurezza del lavoro ha previsto, all'art. 30, che il Modello idoneo ad avere efficacia esimente della responsabilità amministrativa, adottato ed efficacemente attuato, deve assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici previsti:

- al rispetto degli *standard* tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

A tal fine si devono prevedere:

- idonei sistemi di registrazione dell'avvenuta effettuazione delle sopra menzionate attività;
- per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

### **8.3 Sistema dei controlli**

Il sistema dei controlli applicabili all'attività individuata è stato definito sulla base delle indicazioni fornite dalla normativa di settore, nonché dalle best practice in tema di salute dei lavoratori.

Per ognuna delle attività, oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, sono stati individuati i seguenti standard di controllo.

Il Modello prevede l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili.

### **8.3.1 Controlli generali**

I controlli generali sono i seguenti:

#### Separazione delle responsabilità/funzioni/processo

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

#### Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Devono esistere disposizioni aziendali idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività.

#### Sistema deleghe, poteri di firma e poteri autorizzativi

Devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi.

#### Tracciabilità

Deve essere assicurata la tracciabilità della documentazione e delle relative fonti e degli elementi informativi, nonché la relativa archiviazione.

### **8.3.2 Controlli specifici**

Qui di seguito si individuano, i controlli specificatamente individuati per le aree di attività dell'ente che includono l'attività sensibile della sicurezza sul lavoro.

Gli standard di controllo specifici per la normativa qui trattata sono i seguenti:

#### Ispezioni

Il RSPP effettua una visita ispettiva annuale (per i luoghi di lavoro con più di 200 dipendenti la visita è effettuata due volte l'anno), utilizzando una specifica check-list per la verifica sistematica di tutti gli adempimenti previsti dalla legge.

#### Visite sanitarie

Il medico responsabile della sorveglianza sanitaria effettua le visite dei dipendenti secondo la decorrenza prevista dalla legge

#### Monitoraggio del funzionamento del SPP

E' prevista una riunione annuale in tema di verifica della conformità agli obblighi di legge e proposte di miglioramento della qualità dei servizi ai lavoratori alla quale partecipano tutti gli attori del SPP ed i RLS.

#### Report

Tutte le verifiche sono adeguatamente documentate in atti cartacei predisposti in duplice originale, conservati presso la sede dell'ente per eventuali richieste ed accertamenti da parte delle competenti autorità (es. ASL). Una copia è disponibile presso il sito oggetto di verifica.

#### Formazione

Gli interventi formativi diretti a tutti i dipendenti (autoinformazione WBT626), RLS, APP, RSPP ed addetti all'emergenza per l'antincendio ed il pronto soccorso prevedono un sistema di attestazione della frequenza del corso con test di valutazione finale.



## 9. Reati informatici e trattamento illecito di dati

Nella Parte Speciale vengono illustrate le regole di condotta, le modalità di gestione dei processi ed i controlli adottati al fine di prevenire il verificarsi dei delitti previsti dall'art. 24-bis del Decreto.

Tale Parte Speciale va messa in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### 9.1 Analisi delle fattispecie di reato

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d. lgs. n. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal Decreto.

La legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero" ha ampliato le fattispecie di reato che possono generare la responsabilità dell'ente. L'art. 7 del predetto provvedimento ha introdotto nel Decreto l'art. 24-bis "Delitti informatici e trattamento illecito di dati", di seguito individuati:

#### Documenti informatici (art. 491 -bis del codice penale).

"Se alcune delle falsità previste dal presente capo riguardano 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".

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

#### Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)

"Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni";

#### Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)

"Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempite le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni".

#### Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)

"Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni".

#### Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)

“Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476”;

*Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)*

“Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni”;

*Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)*

“Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro”;

*Falsità materiale commessa da privato (art. 482 c.p.)*

“Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo”;

*Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)*

“Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi”;

*Falsità in registri e notificazioni (art. 484 c.p.)*

“Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00”;

*Falsità in scrittura privata (art. 485 c.p.)*

“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata”;

*Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.)*

“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito”;

*Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)*

“Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa

scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480”;

Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)

“Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private”;

Uso di atto falso (art. 489 c.p.)

“Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno”;

Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)

“Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente”;

Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)

“Agli effetti delle disposizioni precedenti, nella denominazione di “atti pubblici” e di “scritture private” sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti”;

Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)

“Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni”.

Accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.)

Commette il delitto 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.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 - quater c.p.)

Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

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.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 - quinquies c.p.)

Commette il delitto 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.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 - quater c.p.)

Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

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.

*Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 -quinqües c.p.)*

Compie il delitto 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.

*Danneggiamento di informazioni, dati e programmi informatici (art. 635 - bis c.p.)*

Il delitto, salvo che il fatto costituisca più grave reato, consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui, da chiunque posta in essere.

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

Il delitto, che può essere commesso da chiunque, consiste, salvo che il fatto costituisca più grave reato, nella commissione di 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.

*Danneggiamento di sistemi informatici e telematici (art. 635 -quater c.p.)*

Il delitto, salvo che il fatto costituisca più grave reato, è commesso da 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.

*Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 - quinqües c.p.)*

Il delitto è commesso se il fatto di cui all'art. 635-quater c.p. 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.

*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 - quinqües c.p.)*

Commette il delitto 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.

## **9.2 Attività sensibili**

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui all'art. 24-bis del Decreto, le aree sensibili di seguito elencate.

### **Gestione dei sistemi informativi e sicurezza logica e fisica**

- Gestione dei profili utente e del processo di autenticazione;
- Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio;

- Gestione e protezione della postazione di lavoro;
- Gestione degli accessi da e verso l'esterno;
- Gestione e protezione delle reti;
- Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD);
- Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.);
- Produzione e/o vendita di programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti.

### **9.3 Sistema dei controlli**

Oltre al rigoroso rispetto del documento denominato "Codice Etico" e delle policy aziendali, sono stati individuati standard di controllo. In particolare, il Modello prevede l'applicazione di:

- Controlli generali: ossia i controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: ossia i controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili;
- Controlli relativi alle attività sensibili sopra individuate, in tutto o in parte affidate a soggetti esterni all'ente.

#### **9.3.1 Controlli generali**

I controlli generali, presenti in ciascuna delle attività sensibili, sono i seguenti:

##### Politiche di sicurezza

Deve essere formalizzata una politica in materia di sicurezza del sistema informativo che preveda, fra l'altro:

- le modalità di comunicazione anche a terzi;
- le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi.

##### Organizzazione della sicurezza per gli utenti interni

Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.

##### Classificazione e controllo dei beni

Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità per l'identificazione e la classificazione degli asset aziendali (ivi inclusi dati e informazioni).

##### Gestione delle comunicazioni e dell'operatività

Deve essere adottato e attuato uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. In particolare, tale strumento normativo deve assicurare:

- il corretto e sicuro funzionamento degli elaboratori di informazioni;
- la protezione da software pericoloso;
- il back-up di informazioni e software;

- la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
- gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
- il controllo sui cambiamenti agli elaboratori e ai sistemi;
- la gestione di dispositivi rimovibili.

#### Audit

Deve essere adottato e attuato uno strumento normativo che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.

#### Risorse umane e sicurezza

Deve essere adottato e attuato uno strumento normativo che preveda:

- la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
- specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
- l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

### **9.3.2 Controlli specifici**

Qui di seguito si individuano, i controlli specificatamente individuati per aree di attività dell'ente che includono le attività sensibili come sopra individuate:

Oltre al rigoroso rispetto del documento denominato Codice Etico e delle policy aziendali, relativamente a tale attività sensibile, gli standard di controllo specifici sono i seguenti:

#### Controllo degli accessi

Deve essere adottato e attuato uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo deve prevedere:

- l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
- le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
- una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;

- la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
- la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
- l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
- la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
- la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
- la custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati.

#### Gestione degli incidenti e dei problemi di sicurezza informatica

Dove essere adottato e attuato uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo deve prevedere:

- appropriati canali gestionali per la comunicazione degli incidenti e problemi;
- l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;
- la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
- l'analisi di report e trend sugli incidenti e sui problemi e l'individuazione di azioni preventive;
- appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
- l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
- l'utilizzo di basi dati informative per supportare la risoluzione degli incidenti;
- la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
- la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.

#### Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi

Deve essere adottato e attuato uno strumento normativo che definisca:

- l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- la confidenzialità, autenticità e integrità delle informazioni;
- la sicurezza nel processo di sviluppo dei sistemi informativi.

#### Organizzazione della sicurezza per gli utenti esterni

Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di

accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

#### Sicurezza fisica e ambientale

Deve essere adottato e attuato uno strumento normativo che disponga l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

#### **9.3.3 Controlli relativi ad attività sensibili affidate, in tutto o in parte, a soggetti esterni all'ente**

Nel caso in cui una delle sopra elencate attività sensibili sia, in tutto o in parte, affidata, in virtù di appositi accordi, a soggetti esterni all'ente, anche appartenenti al medesimo gruppo, il sistema di controllo adottato dall'ente, concerne la previsione, negli accordi e/o nei documenti che disciplinano lo svolgimento di tali attività la previsione di specifiche clausole:

- con cui il terzo dichiara l'impegno a dotarsi di misure idonee a prevenire il rischio di commissione dei reati richiamati dal d. lgs. n. 231/2001, nello svolgimento delle attività per conto dell'ente, che potrebbero essere ascritti all'ente;
- che attribuiscano, quando ritenuto opportuno, all'ente la possibilità di effettuare degli audit per verificarne il rispetto;
- che disciplinino le conseguenze della violazione da parte del terzo delle norme di cui al d. lgs. n. 231/2001 (es. clausola risolutiva espressa, penali) e degli standard concordati nei documenti contrattuali.

## 10. Altri reati

Nella Parte Speciale vengono illustrate le regole di condotta, le modalità di gestione dei processi ed i controlli adottati al fine di prevenire il verificarsi dei delitti previsti nel Decreto.

In particolare:

- Delitti di criminalità organizzata (art. 24-ter d.lgs. 231/01) - Articolo aggiunto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29;
- Delitti contro l'industria e il commercio (art. 25-bis-1 d.lgs. 231/01) - Articolo aggiunto dalla Legge 23 Luglio 2009, n.99, art.15;
- Delitti in materia di violazioni del diritto d'autore (art. 25-nonies d.lgs. 231/01) – Articolo aggiunto dalla Legge 23 luglio 2009 n. 99 , art. 15;
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-noives d.lgs. 231/01) - Articolo aggiunto dalla L. 3 agosto 2009 n. 116, art. 4.

Tale Parte Speciale è in relazione con i principi comportamentali contenuti nelle policy aziendali e nei documenti di compliance specifici che indirizzano i comportamenti dei destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive dell'ente.

### 10.1 Analisi delle fattispecie di reato

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi dell'art. 24-ter e dell'art. 25-bis, 25-nonies e 25-noives del Decreto, riportiamo qui di seguito una descrizione, in forma sintetica, dei reati alla cui commissione da parte di soggetti riconducibili all'ente (ai sensi dell'art. 5 del Decreto) è collegato il regime di responsabilità a carico dello stesso ente:

#### **Delitti di criminalità organizzata (art. 24-ter, D.Lgs. 231/01)**

- *Associazione per delinquere (art. 416 c.p., ad eccezione del sesto comma);*
- *Associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d. lgs 286/1998 (art. 416, sesto comma, c.p.);*
- *Associazione di tipo mafioso (art. 416-bis c.p.);*
- *Tutti i delitti se commessi avvalendosi delle condizioni previste dall'articolo 416-bis c.p. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.*
- *Scambio elettorale politico-mafioso (art. 416-ter c.p.);*
- *Sequestro di persona a scopo di estorsione (art. 630 c.p.);*
- *Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309);*
- *Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle denominate*

*«da bersaglio da sala», o ad emissione di gas, nonché le armi ad aria compressa o gas compressi, sia lunghe sia corte i cui proiettili erogano un'energia cinetica superiore a 7,5 joule, e gli strumenti lanciarazzi, salvo che si tratti di armi destinate alla pesca ovvero di armi e strumenti per i quali la "Commissione consultiva centrale per il controllo delle armi" escluda, in relazione alle rispettive caratteristiche, l'attitudine a recare offesa alla persona. (art. 407, co. 2, lett. a), numero 5), c.p.p.).*

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

- 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.)
- Fabbricazione 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.)

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

##### **Art. 171 l. n. 633/1941**

Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

##### **Art. 171-bis l. n. 633/1941**

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli

articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

Art. 171-ter l. n. 633/1941

1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da da euro 2.582 a euro 15.493 chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

#### Art. 171-septies l. n. 633/1941

1. La pena di cui all'articolo 171-ter, comma 1, si applica anche:

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

#### Art. 171-octies l. n. 633/1941

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi . visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

**Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-novies, D.Lgs. 231/01)**

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

## **10.2 Attività sensibili**

Le analisi svolte hanno permesso di individuare le attività sensibili descritte di seguito.

**Gestione di concessioni, appalti e servizi pubblici**

Acquisizione in modo diretto o indiretto della gestione e controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici.

**Produzione e commercio di prodotti**

Fabbricazione e commercio di prodotti industriali e agroalimentari

**Gestione documenti tutelati dal diritto d'autore**

Riproduzione, duplicazione e diffusione di opere tutelate dal diritto d'autore e da diritti connessi

**Gestione rapporti con autorità giudiziaria**

Gestioni dei rapporti con la magistratura

## **10.3 Sistema dei controlli**

Il sistema di controlli applicabili alle sopra indicate attività sensibili è stato definito utilizzando, come riferimento, le Linee Guida ad oggi pubblicate dalle principali associazioni di categoria nonché le *best practice* internazionali in tema di rischi di frode e corruzione.

Il Modello prevede l'applicazione di:

- Controlli generali: controlli sempre presenti in tutte le attività sensibili;
- Controlli specifici: controlli specificatamente individuati per un'attività sensibile o gruppi di attività sensibili.

### **10.3.1 Controlli generali**

Il Modello contempla l'applicazione dei seguenti controlli generali:

**Segregazione delle attività/funzioni/processo**

Si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza in particolare, nei rapporti che l'ente intrattiene con la Pubblica Amministrazione.

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

Le disposizioni aziendali devono fornire chiari principi generali di riferimento per la regolamentazione dell'attività.

La società provvede alla definizione, alla manutenzione e alla pubblicazione nella Intranet aziendale di tutte le procedure interne, ivi incluse quelle da seguire per la formazione e l'attuazione delle decisioni della società.

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

Si prevede l'obbligo di fissare costantemente ed aggiornare regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma.

#### Tracciabilità

Si richiede l'esistenza di presidi che, in relazione ad ogni comunicazione scritta relativa ai rapporti con la Pubblica Amministrazione in merito a ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

### **10.3.2 Controlli specifici**

Di seguito si individuano gli standard minimi di controllo specificatamente individuati per aree di attività dell'ente che includono le attività sensibili sopra individuate:

#### Obbligo di segnalazione

Deve essere segnalato l'avvio e le fasi più significative di un procedimento o di un rapporto, anche in via mediata, nell'esercizio dell'attività sia ordinaria sia straordinaria, con la Pubblica Amministrazione (partecipazione a procedure di gara o di negoziazione diretta, richiesta di finanziamenti pubblici da parte di organismi nazionali o esteri, ...), specificando la tipologia di operazione, le caratteristiche ed i soggetti esterni coinvolti, in particolar modo se si tratta di enti pubblici. La segnalazione deve contenere una sintetica descrizione delle caratteristiche del rapporto con la Pubblica Amministrazione specificando la tipologia di operazione, le sue caratteristiche ed i soggetti esterni coinvolti, in particolar modo se si tratta di enti pubblici. In ogni caso la segnalazione deve essere conservata, al fine di consentire, in qualunque momento, l'effettuazione di controlli da parte del soggetto destinatario della segnalazione o dell'Organismo di Vigilanza.

#### Autorizzazione formale

Deve esistere un'autorizzazione formalizzata alla stipulazione di un atto formale o all'esecuzione di una operazione.

#### Report

Devono esistere report inviati al superiore gerarchico o al referente interno individuato, dettagliati per ogni singola operazione.

#### Registrazione

L'operazione deve essere registrata e documentata come da procedure aziendali.

#### Sicurezza informatica

Deve essere affidata esclusivamente a una Funzione competente, che ne deve assicurare la tracciabilità la cancellazione di dati, liste di controllo e archivi. Devono esistere liste di controllo degli accessi ai sistemi informativi e automatismi di segnalazione all'amministratore del sistema di operazioni non autorizzate: cancellazioni, tentativi di accesso, alterazione delle funzionalità del sistema. I responsabili del monitoraggio del sistema informatico aziendale e della sua revisione censiranno e verificheranno periodicamente:

- le persone che hanno accesso ai mezzi informatici, con particolare riferimento a quanti utilizzano mezzi destinati al contatto con l'esterno (trasmissione dei dati tramite comunicazioni telematiche o informatiche, in modo particolare se questi sono corredati di autenticazione o firma digitale, invio di file prodotti da elaborazioni on line o batch, ...);
- le procedure che producono i dati aziendali, con particolare riferimento a quelle che inviano informazioni aventi rilevanza all'esterno.

Rispetto alle prescrizioni del Modello, permane la validità delle disposizioni definite nelle procedure di maggiore tutela previste nell'ambito aziendale per lo svolgimento delle attività sensibili.

## **Allegati**

L'allegato sintetizza le attività sensibili riferite ai reati attualmente presenti nel Decreto, con l'evidenza dell'applicabilità relativa al contesto di riferimento per ogni Società del Gruppo.

### **Attività sensibili- dettaglio per Società del Gruppo**

**REATI PUBBLICA AMMINISTRAZIONE**

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl
PAM-1	Negoziazione, stipulazione, esecuzione contratti o convenzioni con pubbliche amministrazioni mediante procedure negoziate (affidamento o trattativa privata)."	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile
PAM-2	Negoziazione, stipulazione ed esecuzione contratti o convenzioni con pubbliche amministrazioni ai quali si perviene mediante procedure ad evidenza pubblica (aperte o ristrette).	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile
PAM-3	Liquidazione dei sinistri a favore o per conto di pubbliche amministrazioni	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile
PAM-4	Gestione dei contenziosi giudiziali e stragiudiziali con personale dipendente ed ex dipendente e collaboratori esterni.	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-5	Gestione dei contenziosi giudiziali e stragiudiziali con la clientela.	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Applicabile
PAM-6	Gestione dei rapporti con la pubblica amministrazione per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (D.Lgs. 81/08 e successive modificazioni/integrazioni)	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-7	Amministrazione e gestione del personale	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-8	Rapporti con enti previdenziali e assistenziali	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-9	Rapporti con Autorità di Vigilanza relativi allo svolgimento di attività regolate dalla normativa di riferimento e gestione dei rapporti per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali.	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Applicabile
PAM-10	Gestione dei rapporti con l'amministrazione finanziaria	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-11	Promozioni commerciali e sponsorizzazioni a pubbliche amministrazioni.	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Applicabile
PAM-12	Acquisizione e/o gestione di contributi, sovvenzioni e finanziamenti concessi da pubbliche amministrazioni.	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-13	Ogni possibilità di detenere, maneggiare o utilizzare denaro/valori di bollo, disponibilità di fondi	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PAM-14	Gestione di software di pubbliche amministrazioni o forniti da terzi per conto di pubbliche amministrazioni e collegamenti telematici (in entrata/uscita) o trasmissione di dati su supporti informatici a pubbliche amministrazioni, enti pubblici o autorità	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile

## REATI SOCIETARI

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
SOC-1	Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza.	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
SOC-2	Predisposizione di prospetti relativi alla sollecitazione, all'investimento, al pubblico risparmio e/o di ammissione alla quotazione in mercati regolamentati e non regolamentati e/o operazioni straordinarie sul capitale (opa, opv, ops, ecc.)	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile
SOC-3	Gestione dei rapporti con la società di revisione, collegio sindacale e altri organi societari e relativa redazione, tenuta e conservazione dei documenti su cui gli stessi possono esercitare il controllo.	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
SOC-4	Attività di preparazione delle riunioni assembleari	Non Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
SOC-5	Comunicazione degli interessi degli amministratori	Non Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
SOC-6	Gestione delle incombenze societarie; operazioni sul capitale e operazioni su azioni e quote	Non Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile

## GESTIONE RISORSE FINANZIARIE

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
FIN-1	Gestione delle risorse finanziarie	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile

### ABUSI DI MERCATO

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
ABM-1	Gestione delle informazioni privilegiate	Non applicabile	Non applicabile	Non applicabile	Non applicabile	Non applicabile	Non applicabile
ABM-2	Predisposizione e comunicazione di notizie/ dati verso l'esterno	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Non applicabile
ABM-3	Gestione di attività di negoziazione di strumenti finanziari	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Non applicabile

### ANTITERRORISMO

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
TER-1	Adempimenti antiterrorismo	Non Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile	Applicabile
TER-2	Gestione di iniziative umanitarie e di solidarietà in favore di enti con sede o operanti in paesi considerati a rischio	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile

### ANTIRICICLAGGIO

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
ARC-1	Attività di vendita di prodotti finanziari e di altri servizi legati agli investimenti	Non Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile	Applicabile
ARC-2	Rapporti con controparti per l'acquisto di beni e/o servizi di importo rilevante e gli investimenti	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile

### PERSONALITA' INDIVIDUALE

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
PEI-1	Promozione e/o gestione di iniziative umanitarie e di solidarietà	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Applicabile
PEI-2	Gestione siti internet e intranet	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
PEI-3	Organizzazione e promozione di viaggi (viaggi premio) per dipendenti o partner commerciali	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Non Applicabile
PEI-4	Attività che coinvolgono direttamente minorenni, soprattutto per finalità didattiche, sportive e ricreative	Applicabile	Applicabile	Applicabile	Applicabile	Non Applicabile	Applicabile

### SICUREZZA SUL LAVORO

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
SIC-1	Sicurezza e igiene sul lavoro (D.Lgs. 81/08 e successive modificazioni/integrazioni).	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile

### REATI INFORMATICI

Codice	Attività sensibile	Helvetia Assicurazioni SA	Helvetia Vita SpA	Chiara Vita SpA	Padana Assicurazioni SpA	GE.SI.ASS Srl	APSA Srl;
INF-1	Gestione dei sistemi informativi e sicurezza logica e fisica.	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile

**ALTRI REATI**

<b>Codice</b>	<b>Attività sensibile</b>	<b>Helvetia Assicurazioni SA</b>	<b>Helvetia Vita SpA</b>	<b>Chiara Vita SpA</b>	<b>Padana Assicurazioni SpA</b>	<b>GE.SI.ASS Srl</b>	<b>APSA Srl;</b>
CRO	Gestione di concessioni, appalti e servizi pubblici	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile
ICO	Produzione e commercio di prodotti	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile	Non Applicabile
DDA	Gestione documenti tutelati dal diritto d'autore	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile
AGI	Gestione rapporti con Autorità Giudiziaria	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile	Applicabile