

DOCUMENTO ILLUSTRATIVO DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Aviva Italia Holding S.p.A.

Ai sensi dell'art. 6, comma 1,
lett. a) del Decreto Legislativo
n. 231 dell'8 giugno 2001

EDIZIONE 2011



Indice

Definizioni.....	4
Parte Generale	6
Premessa.....	6
1. Contesto normativo di riferimento.....	6
1.1 La disciplina della responsabilità amministrativa.....	6
1.2 I reati presupposto.....	8
1.3 Elementi chiave del Decreto.....	11
1.4 Autori del reato	12
1.5 Natura della responsabilità	12
1.6 Le sanzioni previste.....	12
1.7 La responsabilità della società	14
1.8 Soggetti in posizione apicale.....	14
1.9 Soggetti sottoposti a direzione o vigilanza del soggetto apicale	15
2. Attività e organizzazione.....	16
2.1 Aspetti Organizzativi.....	16
2.2 Governance e sistema di controllo interno	18
2.3 Valori di riferimento e normativa interna.....	19
3. Il Modello di organizzazione, gestione e controllo.....	20
3.1 Adozione del Modello	20
3.2 Linee Guida di categoria.....	20
3.3 Definizione del Modello	23
3.4 Gli elementi base.....	24
3.5 La struttura del Modello	25
3.6 Comunicazione ai dipendenti	26
4. L'Organismo di Vigilanza.....	28
4.1 Identificazione dell'Organismo di Vigilanza	28
4.2 Caratteristiche dell'Organismo di Vigilanza	28
4.3 Composizione	28
4.4 Nomina, revoca e sostituzione	29
4.5 Funzionamento	31
4.6 Funzioni e poteri	32
4.7 Modalità di interazione con le altre funzioni aziendali	33
4.8 La gestione delle segnalazioni	34
4.9 Flusso di informazioni verso l'Organismo di Vigilanza	34
4.10 Reporting dell'Organismo di Vigilanza	34
4.11 I controlli dell'Organismo di Vigilanza.....	35
4.12 Raccolta e conservazione delle informazioni	37
5. Il sistema disciplinare e sanzionatorio.....	38
5.1 Disciplina sanzionatoria.....	38
5.2 Accertamento della violazione.....	38
5.3 Misure nei confronti dei dipendenti non dirigenti	39
5.4 Misure nei confronti dei dipendenti dirigenti	39
5.5 Misure nei confronti dei collaboratori esterni, intermediari e dei partner commerciali	40

5.6 Misure nei confronti degli Amministratori	40
5.7 Misure nei confronti dei Sindaci.....	40
Parte Speciale	41
1. Reati contro la Pubblica Amministrazione	41
1.1 Analisi delle fattispecie di reato	41
1.2 Attività sensibili	47
1.3 Sistema dei controlli	49
2. Reati societari	52
2.1 Analisi delle fattispecie di reato	52
2.2 Attività sensibili	57
2.3 Sistema dei controlli	58
3. Gestione delle risorse economiche e finanziarie	63
3.1 Attività sensibili	63
3.2 Sistema dei controlli	63
4. Abusi di mercato.....	66
4.1 Analisi delle fattispecie di reato	66
4.2 Attività sensibili	71
4.3 Sistema dei controlli	71
5. Reati di ricettazione, riciclaggio e impiego di denaro, di beni o di utilità di provenienza illecita	76
5.1 Analisi delle fattispecie di reato	76
5.2 Attività sensibili	77
5.3 Sistema dei controlli	77
6. Reati con finalità di terrorismo o di eversione dell'ordine democratico	80
6.1 Analisi delle fattispecie di reato	80
6.2. Attività sensibili	81
6.3 Sistema dei controlli interni.....	82
7. Delitti contro la personalità individuale	85
7.1 Analisi delle fattispecie di reato	85
7.2 Attività sensibili	87
7.3 Sistema dei controlli	88
8. Sicurezza sul lavoro	91
8.1 Analisi delle fattispecie di reato	91
8.2 Attività sensibili	92
8.3 Sistema dei controlli	94
9. Reati informatici e trattamento illecito di dati	97
9.1 Analisi delle fattispecie di reato	97
9.2 Attività sensibili	100
9.3 Sistema dei controlli	101
10. Altri reati	106
10.1 Analisi delle fattispecie di reato	106
10.2 Attività sensibili	115
10.3 Sistema dei controlli	115

Definizioni

- **“Attività Sensibili”**: attività aziendali esposte alla potenziale commissione dei reati contemplati dalla normativa e richiamati dal d. lgs. n. 231/2001.
- **“Capogruppo”**: Aviva Italia Holding S.p.A.;
- **“Codice Etico”**: Codice Etico del Gruppo Aviva 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 per la società (cd. lavoratori somministrati) e i dipendenti distaccati da altre Società;
- **“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 (es. Responsabile dell’Ufficio).
- **“Modello di organizzazione, gestione e controllo”** o **“Modello”**: il Documento Illustrativo del Modello di Organizzazione, Gestione e Controllo e tutte le norme predisposte ai fini del Sistema di Controllo Interno a presidio del d. lgs. 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”**: Consiglio di Amministrazione;
- **“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; società che debbono obbligatoriamente procedere alla stipulazione di contratti di fornitura di servizi attraverso il ricorso a gare d’appalto;

- **“Società”**: Aviva Italia Holding S.p.A.;
- **“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

Premessa

Il Gruppo Aviva Italia ha provveduto ad elaborare il “Documento Illustrativo del Modello di Organizzazione, Gestione e Controllo” con riferimento alle “Linee Guida per il settore assicurativo in materia di responsabilità amministrativa” e relativi suggerimenti operativi predisposti dalla Associazione di categoria (ANIA) e alle *best practice* di mercato.

Il presente documento è composto da una Parte Generale e una Parte Speciale.

La Parte Generale descrive lo scenario normativo di riferimento, le informazioni generali relative al profilo organizzativo del Gruppo Aviva Italia, il processo di definizione, i principi di attuazione e funzionamento del Modello e il sistema sanzionatorio.

La Parte Speciale descrive l'analisi normativa svolta relativamente ai reati previsti nel d. lgs 231/2001, le attività sensibili alla commissione dei reati, il sistema dei controlli che prevede controlli generali e controlli specifici e i principi procedurali.

I destinatari sono tenuti alla conoscenza ed osservanza dei principi contenuti nel presente documento, la cui diffusione viene assicurata nei confronti dei lavoratori subordinati, amministratori, sindaci ed altri destinatari attraverso la pubblicazione sulla intranet aziendale e nei confronti degli enti esterni che interagiscono in maniera continuativa e strutturata con le Società del Gruppo attraverso la pubblicazione sul sito internet aziendale.

1. Contesto normativo di riferimento

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. 300¹, disciplina la “*responsabilità degli enti per gli illeciti amministrativi dipendenti da reato*”, che si

¹ 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).

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)² 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.

Gli aggiornamenti normativi relativi al D.Lgs. 231/01 sono i seguenti:

- Il **D.L. 25 settembre 2001, n. 350**, convertito con L. 23 novembre 2001, n. 409 ha disposto (art. 6) l'introduzione dell'art. **25–bis**.
- Il **D.Lgs. 11 aprile 2002, n. 61** ha disposto (art. 3) l'introduzione dell'art. **25–ter** e la seguente modifica nel Capo I, Sezione III: la partizione "Responsabilità amministrativa per reati previsti dal codice penale" è sostituita dalla seguente: "Responsabilità amministrativa da reato".
- Il **D.P.R. 30 maggio 2002, n. 115** ha disposto (art. 299) l'abrogazione dell'art. **75**.
- La **L. 14 gennaio 2003, n. 7** ha disposto (art. 3) l'introduzione dell'art. **25–quater**.
- Il **D.P.R. 14 novembre 2002, n. 313** ha disposto (art. 52 (L)) la modifica dell'art. **85** e l'abrogazione degli artt. **80, 81 e 82**.
- Il **D. 26 giugno 2003, n. 201** precisa che (art. 8), rispetto ai termini stabiliti dall'art. 6 del d.lgs. 231/01, "Per i codici di comportamento inviati al Ministero della giustizia fino alla data di entrata in vigore del presente regolamento, il termine di trenta giorni di cui all'articolo 6, comma 3, del decreto legislativo n. 231 del 2001, decorre da tale data."
- La **L. 11 agosto 2003, n. 228** ha disposto (art. 5) l'introduzione dell'art. **25–quinquies**.

² 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)*".

- La **L. 18 aprile 2005, n. 62** ha disposto (art. 9) l'introduzione dell'art. **25–sexies**.
- La **L. 28 dicembre 2005, n. 262** ha disposto (art. 31) la modifica dell'art. **25–ter**.
- La **L. 9 gennaio 2006, n. 7** ha disposto (art. 8) l'introduzione dell'art. **25–quater.1**.
- La **L. 6 febbraio 2006, n. 38** ha disposto (art. 10) la modifica dell'art. **25–quinquies**.
- La **L. 3 agosto 2007, n. 123** ha disposto (art. 9) l'introduzione dell'art. **25–septies**.
- Il **D.Lgs. 21 novembre 2007, n.231** ha disposto (art. 63) l'introduzione dell'art. **25–octies**.
- La **L. 18 marzo 2008, n. 48** ha disposto (art. 7) l'introduzione dell'art. **24–bis**.
- Il **D.Lgs. 9 aprile 2008, n. 81** ha disposto (art. 300) la modifica dell'art. **25–septies**.
- La **L. 15 luglio 2009, n. 94** ha disposto (art. 2) l'introduzione dell'art. **24–ter**.
- La **L. 23 luglio 2009, n. 99** ha disposto (l'art. 15, comma 7) la modifica dell'art. **25–bis**, commi 1, 2 e rubrica, l'introduzione degli artt. **25–bis.1** e **25–novies**.
- La **L. 3 agosto 2009, n. 116** ha disposto (art. 4) l'introduzione di un “secondo” art. **25–novies**.

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 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. 27 D. Lgs. 39/2010), 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, ritenuta 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*³ 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*⁴ 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 dati⁵;

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

- **delitti di criminalità organizzata.** L'art. 24–ter del Decreto prevede fattispecie di reato in materia di sicurezza pubblica⁶;
- **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 industriale⁷;
- **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 autore⁸;
- **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 giudiziaria⁹.

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,

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, *Cybercrime 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).

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

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 terzi¹⁰.

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 Costituzione¹¹, ma con numerosi punti di contatto con una responsabilità di tipo penale.

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

¹⁰ 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”*.

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

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"¹² 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 società¹³, 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;

¹² D. lgs. n. 231/2001, artt. 10 – 12.

¹³ 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".

- 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.

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 requisiti sotto elencati (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

Struttura del Gruppo

Il Gruppo Aviva in Italia, risulta al 31 dicembre 2010 così composto:

- una holding assicurativa e capogruppo del Gruppo Aviva in Italia:
 - Aviva Italia Holding S.p.A.
- una sub–holding di partecipazioni finanziarie:
 - Petunia S.p.A.
- sei imprese di assicurazioni di diritto italiano operanti nel settore vita:
 - Aviva S.p.A.
 - Aviva Vita S.p.A.
 - Aviva Life S.p.A.
 - Aviva Previdenza S.p.A.
 - Aviva Assicurazioni Vita S.p.A.
 - Avipop Vita S.p.A.
- un'impresa di assicurazione di diritto irlandese operante nel settore vita:
 - Area Life International Assurance Ltd
- tre imprese di assicurazioni operanti nel settore danni:
 - Aviva Italia S.p.A.;
 - Aviva Assicurazioni S.p.A.;
 - Avipop Assicurazioni S.p.A.

La società **Area Life International Assurance Limited** è partecipata da Aviva Italia Holding S.p.A per il 55 per cento e per il 45 per cento da Sopaf S.p.A. L'impresa, con sede legale in Irlanda, Dublino, autorizzata all'esercizio dell'attività assicurativa come da autorizzazione rilasciata dalle competenti Autorità irlandesi, opera in Italia in regime di stabilimento.

La sub–holding, **Petunia S.p.A.** – partecipata per il 51 per cento dei diritti di voto da Aviva Italia

Holding S.p.A. e per il restante 49 per cento di tali diritti da Sopaf S.p.A., detiene a sua volta il 49,99 per cento del capitale sociale di Banca Network Investimenti S.p.A. (già Banca Bipielle Network S.p.A.).

A completamento delle informazioni riportate nei precedenti paragrafi, il Gruppo detiene, per il tramite di **Finoa s.r.l.** una partecipazione rilevante nella società **Eurovita Assicurazioni S.p.A.** Tale società che, per effetto della composizione azionaria e delle situazioni che hanno progressivamente mutato il quadro di riferimento delineato nella precedente relazione in forza dei quali non sussistono più i presupposti necessari ad esercitare l'attività di direzione e coordinamento del Gruppo Aviva sulla società, presenta un profilo operativo e gestionale autonomo rispetto alle altre imprese del Gruppo Aviva in Italia aventi sede in Milano e strutturalmente parte del medesimo modello organizzativo – gestionale.

La Società

La società Aviva Italia Holding S.p.A., costituita nell'esercizio 2001 per mezzo di scissione da Commercial Union Italia S.p.A. ora Aviva Italia S.p.A., è interamente posseduta da Aviva Europe SE.

La società Aviva Italia Holding S.p.A. fornisce servizi alle altre imprese del Gruppo Aviva nel rispetto di specifici contratti di prestazione di servizi in outsourcing.

Le attività oggetto di appositi contratti di servizio fanno riferimento alle seguenti aree funzionali: servizi di Direzione Generale, risk management, compliance, internal audit, reporting e controllo di gestione, amministrazione, contabilità agenzie, legale societario, servizio fiscale, servizi informativi, risorse umane, servizi generali, servizi attuariali, gestione reclami, sviluppo competitivo, marketing.

Al riguardo si ritiene opportuno sottolineare che i servizi prestati da società del Gruppo Aviva in Italia – tenuto conto del modello organizzativo del Gruppo medesimo – sono da ritenersi ispirati ad una logica di centralizzazione di servizi comuni ivi incluse le funzioni di Risk Management, Internal Audit e Compliance.

Il sistema di controllo interno e la gestione del profilo di rischio nonché la funzione di Compliance inerente alle singole imprese componenti il Gruppo Aviva in Italia è attuato mediante un processo di direzione e coordinamento operato dalla Capogruppo Aviva Italia Holding S.p.A. attraverso le proprie strutture dedicate alla pianificazione ed alla successiva gestione di tali attività che trovano specifica regolamentazione nell'ambito dei contratti in precedenza richiamati.

Ai sensi dell'art. 2497 del Codice Civile, Aviva Italia Holding S.p.A. esercita attività di Direzione e Coordinamento sulle seguenti società facenti parte del Gruppo Aviva:

- Aviva Italia S.p.A.

- Aviva Assicurazioni S.p.A.
- Aviva S.p.A.
- Aviva Life S.p.A.
- Aviva Previdenza S.p.A.
- Aviva Vita S.p.A.
- Aviva Assicurazioni Vita S.p.A
- Avipop Assicurazioni S.p.A.
- Avipop Vita S.p.A.

Il rispetto di tale impostazione garantisce la coerenza e l'efficacia dei sistemi di controllo posti in essere in tutte le imprese appartenenti al Gruppo Aviva in Italia. Risultano inoltre parte integrante dei principi in precedenza richiamati quelle attività – laddove esistenti – attribuite in gestione esterna (outsourcing).

Al riguardo, si segnala che la società ha definito la politica di esternalizzazione delle attività della Capogruppo a valere su tutte le società del Gruppo Aviva in Italia, mediante delibera assunta dal Consiglio di Amministrazione di Aviva Italia Holding S.p.A. e conseguentemente approvata da tutte le Compagnie del Gruppo Aviva in Italia e redatta in ottemperanza a quanto disposto dall'art. 31 del Regolamento ISVAP n. 20/2008.

2.2 Governance e sistema di controllo interno

La Governance della Società costituisce uno degli aspetti fondamentali per garantire l'efficacia del Modello, in quanto inerente agli aspetti relativi alla ripartizione dei poteri e delle responsabilità tra gli organi sociali e le funzioni aziendali.

L'Organo Amministrativo è investito per Statuto dei più ampi poteri di ordinaria e straordinaria amministrazione ed, in particolare, definisce le strategie e le politiche generali di gestione della Società.

L'Organo Amministrativo esamina ed approva l'assetto organizzativo aziendale coerentemente con gli obiettivi strategici e le politiche aziendali, avendo cura che sia attuata una appropriata separazione di funzioni e poteri. La sua rappresentazione viene comunicata attraverso l'organigramma aziendale e reso operativo dall'Amministratore Delegato; le modifiche sono tempestivamente comunicate a tutta la struttura organizzativa attraverso specifiche comunicazioni organizzative interne.

Coerentemente con il Regolamento n. 20 del 26 marzo 2008, la Capogruppo ha 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.

Il Collegio Sindacale in attuazione dei propri doveri istituzionali di controllo di legalità e di gestione, verificano l'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla Società e il suo concreto funzionamento, valutano l'efficienza e l'efficacia del sistema dei controlli interni e segnalano all'Organo Amministrativo le eventuali anomalie o debolezze dell'assetto organizzativo e del sistema dei controlli interni indicando e sollecitando idonee misure correttive, prendendo visione anche dei risultati dei lavori effettuati da quanti svolgono attività di controllo nella Società.

L'Audit Committee, in attuazione delle proprie funzioni consultive e propositive di cui all'Art 6 del Regolamento ISVAP n. 20 assiste l'Organo Amministrativo nella determinazione delle linee d'indirizzo del Sistema dei controlli interni, nella verifica periodica della sua adeguatezza e del suo effettivo funzionamento, nell'identificazione e gestione dei principali rischi aziendali.

2.3 Valori di riferimento e normativa interna

I valori di riferimento sono diffusi attraverso Codice Etico e *Policies* specifiche che indirizzano i comportamenti di dipendenti e 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 Società, 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.

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 della Società, 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 2¹⁴, 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"*.

¹⁴ Art. 6, comma 2, del d. lgs. 231/2001: "In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze:

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

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 valutare 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 proporre 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;
- 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 un 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, sulle componenti del modello adottato e in materia di responsabilità organizzativa e gestionale.

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 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 stati descritti i controlli previsti e le funzioni coinvolte nei processi.

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 portato 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 e le seguenti aree di rischio:

- “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 “transnazionalità”, 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 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 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 Comunicazione ai dipendenti

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, l'Organo Amministrativo della Società ha 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 all'Organo Amministrativo della Società 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.

La scelta operata deve essere ispirata al principio di nominare quali componenti dell'Organismo coloro i quali siano in possesso di competenze e conoscenze che garantiscano il miglior contributo, 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 all'Organo Amministrativo della Società, il quale nomina sulla base dei criteri enunciati.

Il Presidente dell'Organismo è nominato e revocato dall'Organo Amministrativo della Società; in mancanza, il Presidente dell'Organismo viene eletto dal medesimo Organismo di Vigilanza. E'facoltà dell'Organismo di nominare un Segretario, scegliendolo anche al di fuori dei suoi componenti.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza dei requisiti soggettivi di eleggibilità. L'Organo Amministrativo della Società, in sede di nomina, deve 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 Amministrativo (salvo che si tratti di amministratori non esecutivi o non esecutivi indipendenti, come individuati dall'art. 2387 cod. civ. e dall'art. 3 del Codice di autodisciplina delle società quotate [1]) 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;

[1] Nel quadro della revisione del Codice di autodisciplina, gli amministratori indipendenti vengono definiti come "amministratori non esecutivi ... che non intrattengono, né hanno di recente intrattenuto, neppure indirettamente, con l'emittente o con soggetti legati all'emittente, relazioni tali da condizionarne attualmente l'autonomia di giudizio".

- 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 l'Organo Amministrativo della Società 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 l'Organo Amministrativo della Società al fine di procedere alla sostituzione.

I componenti dell'Organismo sono revocati immediatamente dall'Organo Amministrativo della Società 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, l'Organo Amministrativo della Società provvede tempestivamente alla sostituzione del componente revocato.

In caso di dimissione di uno o più componenti, l'Organo Amministrativo della Società procede 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 l'Organo Amministrativo della Società provvede, 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

L'Organismo di Vigilanza si riunisce almeno con cadenza trimestrale. E' inoltre convocato dal Presidente ogniqualvolta il medesimo ne ravvisi la necessità, nel luogo fissato, a mezzo di apposito avviso trasmesso a tutti i componenti. L'Organismo è inoltre convocato dal Presidente qualora ne faccia richiesta anche uno solo dei componenti. La convocazione viene effettuata almeno due giorni liberi prima di quello fissato per l'adunanza, con ogni mezzo ritenuto idoneo a garantire una comunicazione certa ed immediata. In caso di urgenza, il termine può essere ridotto ad un giorno libero. L'avviso di convocazione contiene il luogo, il giorno, l'ora della riunione e l'elenco delle materie da trattare. Per la validità della costituzione di ogni seduta, occorre la

presenza della maggioranza dei componenti in carica. Le deliberazioni sono prese a maggioranza assoluta di voti. Di ogni adunanza viene redatto apposito verbale, sottoscritto dal Presidente e dal Segretario. Le riunioni possono tenersi nella sede sociale della Società o in altro luogo indicato nell'avviso di convocazione. E' ammessa la possibilità che le stesse possano tenersi in videoconferenza o in audioconferenza, a condizione che tutti i partecipanti siano in grado di identificarsi tra loro, che sia loro consentito di seguire la discussione e di intervenire in tempo reale nella trattazione degli argomenti discussi, che sia loro consentito lo scambio di documenti relativi a tali argomenti e che ne venga dato atto nel relativo verbale. In tale casistica, la riunione dell'Organismo si considera tenuta nel luogo in cui si trovano il Presidente ed il Segretario.

4.6 Funzioni e poteri

L'Organo Amministrativo della Società, in coerenza con i principi sanciti dal d. lgs. n. 231/01, affida 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 l'Organo Amministrativo della Società 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:
 - Ufficio Legale e Societario (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 e Finanza (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 puntuale dell'Organismo di Vigilanza con 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 della Società, gli amministratori, i sindaci e i revisori esterni 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 l'Organismo di Vigilanza, secondo le modalità che esso avrà cura di specificare o attraverso il servizio "Right Call".

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.

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 e i collaboratori interni ed esterni 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 l'Organo Amministrativo della Società.

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 annuale e comunque 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:

- 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 sull'attuazione del Modello, 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 la Società ha 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;
 - 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 in materia di antiriciclaggio:

- l'obbligo di vigilare sull'osservanza delle norme contenute nel d. lgs. n. 231/2007;
- specifici obblighi di comunicazione, a rilevanza sia meramente interna che esterna. In particolare questo deve:
 - a) comunicare, senza ritardo, alle Autorità di Vigilanza di settore 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, relativamente agli obblighi di adeguata verifica del cliente, l'organizzazione, la registrazione, le procedure e i controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria;
 - b) comunicare, senza ritardo, all'Organo Amministrativo della Società, le infrazioni alle disposizioni di cui all'art. 41 d. lgs. n. 231/2007 di cui abbia notizia, in materia di segnalazioni di operazioni sospette;
 - c) comunicano, entro trenta giorni, all'Autorità di Vigilanza di settore le infrazioni alle disposizioni contenute nell'articolo 36 di cui hanno notizia, in materia di obblighi di

registrazione delle informazioni acquisite per assolvere gli adempimenti di adeguata verifica.

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, descritto nel Modello e nel Regolamento Aziendale, previsto nei confronti dei dipendenti viene costantemente monitorato dalle Risorse Umane.

Poiché l'applicazione delle sanzioni disciplinari 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 la Società.

Si sottolinea che i dipendenti che operano in regime di distacco, anche parziale, da altre Società devono attenersi ai disposti del Modello della Società per la quale prestano la propria attività lavorativa, oltre che di quello adottato dalla Società di appartenenza.

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 da parte delle Risorse Umane, 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 l'Organo Amministrativo della Società, la Compliance 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:

- Disciplina dei rapporti fra le imprese di assicurazione e il personale dipendente non dirigente;
- Contratto nazionale normativo ed economico per i dirigenti delle imprese assicuratrici.

5.3 Misure nei confronti dei dipendenti non dirigenti

Le sanzioni irrogabili nei confronti dei lavoratori dipendenti non dirigenti, 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 degli Amministratori

Ove da verifiche emergessero violazioni o tentativi di violazione del Modello riconducibili agli Amministratori della Società, l'Organismo di Vigilanza ne darà notizia all'Organo Amministrativo, affinché si provveda ad assumere, ciascuno per le proprie rispettive competenze, le iniziative previste dalla vigente normativa.

5.7 Misure nei confronti dei Sindaci

In caso di violazione del presente Modello da parte di uno o più Sindaci, l'Organismo informa l'intero Collegio Sindacale e l'Organo Amministrativo, che prenderanno gli opportuni provvedimenti.

Parte Speciale

La Parte Speciale contiene i risultati dell'analisi delle fattispecie di reato, l'identificazione delle attività sensibili, la definizione dei presidi di controllo e dei principi procedurali.

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 nelle procedure interne, 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:

A. Concussione e corruzione

Concussione (Art. 317 c.p.)

Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, abusando della sua qualità o dei suoi poteri costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da quattro a dodici anni.

Corruzione per un atto d'ufficio (Art. 318 c.p.)

Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a tre anni. Se il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto, la pena è della reclusione fino a un anno.

Corruzione per un atto contrario ai doveri d'ufficio (Art. 319 c.p.)

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

Circostanze aggravanti (Art. 319-bis c.p.)

La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

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

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da tre a otto anni. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da quattro a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni.

Corruzione di persona incaricata di un pubblico servizio (Art. 320)

Le disposizioni dell'articolo 319 si applicano anche all'incaricato di un pubblico servizio; quelle di cui all'articolo 318 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato. In ogni caso, le pene sono ridotte in misura non superiore a un terzo.

Pene per il corruttore (Art. 321 c.p.)

Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.

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

Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, per indurlo a compiere un atto del suo ufficio, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo. Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo. La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di

un pubblico servizio che riveste la qualità di pubblico impiegato che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 318. La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

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

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche: 1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee; 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee; 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee; 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee; 5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio. Le disposizioni degli articoli 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso: 1) alle persone indicate nel primo comma del presente articolo; 2) 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 o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali. Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

B. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico.

Malversazione a danno dello Stato (art. 316-bis c.p.)

Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.

Indebita percezione di erogazioni in danno dello Stato (art. 316-ter c.p.)

Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a euro 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da euro 5.164 a euro 25.822. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

Truffa (Art. 640 c.p.)

Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.

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

La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

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

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

C. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (Art. 453 c.p.)

È punito con la reclusione da tre a dodici anni e con la multa da euro 516 a euro 3.098:

1. chiunque contraffà monete nazionali o straniere, aventi corso legale nello Stato o fuori;
2. chiunque altera in qualsiasi modo monete genuine, col dare ad esse l'apparenza di un valore superiore;
3. chiunque, non essendo concorso nella contraffazione o nell'alterazione, ma di concerto con chi l'ha eseguita ovvero con un intermediario, introduce nel territorio dello Stato o detiene o spende o mette altrimenti in circolazione monete contraffatte o alterate;
4. chiunque, al fine di metterle in circolazione, acquista o comunque riceve, da chi le ha falsificate, ovvero da un intermediario, monete contraffatte o alterate.

Alterazione di monete (Art. 454 c.p.)

Chiunque altera monete della qualità indicata nell'articolo precedente, scemandone in qualsiasi modo il valore, ovvero, rispetto alle monete in tal modo alterate, commette alcuno dei fatti indicati nei n. 3 e 4 del detto articolo, è punito con la reclusione da uno a cinque anni e con la multa da euro 103 a euro 516.

Spendita e introduzione nello Stato, senza concerto, di monete falsificate (Art. 455 c.p.)

Chiunque, fuori dei casi previsti dai due articoli precedenti, introduce nel territorio dello Stato, acquista o detiene monete contraffatte o alterate, al fine di metterle in circolazione, ovvero le spende o le mette altrimenti in circolazione, soggiace alle pene stabilite nei detti articoli, ridotte da un terzo alla metà.

Spendita di monete falsificate ricevute in buona fede (Art. 457 c.p.)

Chiunque spende, o mette altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede, è punito con la reclusione fino a sei mesi o con la multa fino a euro 1.032.

Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (Art. 459 c.p.)

Le disposizioni degli articoli 453, 455 e 457 si applicano anche alla contraffazione o alterazione di valori di bollo e alla introduzione nel territorio dello Stato, o all'acquisto, detenzione e messa in circolazione di valori di bollo contraffatti; ma le pene sono ridotte di un terzo. Agli effetti della legge penale, si intendono per valori di bollo la carta bollata, le marche da bollo, i francobolli e gli altri valori equiparati a questi da leggi speciali.

Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (Art. 460 c.p.)

Chiunque contraffà la carta filigranata che si adopera per la fabbricazione delle carte di pubblico credito o dei valori di bollo, ovvero acquista, detiene o aliena tale carta contraffatta, è punito, se il fatto non costituisce un più grave reato, con la reclusione da due a sei anni e con la multa da euro 309 a euro 1.032.

Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (Art. 461 c.p.)

Chiunque fabbrica, acquista, detiene o aliena filigrane, programmi informatici o strumenti destinati esclusivamente alla contraffazione o alterazione di monete, di valori di bollo o di carta filigranata è punito, se il fatto non costituisce un più grave reato, con la reclusione da uno a cinque anni e con la multa da euro 103 a euro 516. La stessa pena si applica se le condotte previste dal primo comma hanno ad oggetto ologrammi o altri componenti della moneta destinati ad assicurare la protezione contro la contraffazione o l'alterazione.

Uso di valori di bollo contraffatti o alterati (Art. 464 c.p.)

Chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo contraffatti o alterati è punito con la reclusione fino a tre anni e con la multa fino a euro 516. Se i valori sono stati ricevuti in buona fede, si applica la pena stabilita nell'articolo 457, ridotta di un terzo.

Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (Art. 473 c.p.)

Chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.500 a euro 25.000. Soggiace alla pena della reclusione da uno a quattro anni e della multa da euro 3.500 a euro 35.000 chiunque contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati. I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

Introduzione nello Stato e commercio di prodotti con segni falsi (Art. 474 c.p.)

Fuori dei casi di concorso nei reati previsti dall'articolo 473, chiunque introduce nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati è punito con la reclusione da uno a quattro anni e con la multa da euro 3.500 a euro 35.000. Fuori dei casi di concorso nella contraffazione, alterazione, introduzione nel territorio dello Stato, chiunque detiene per la vendita, pone in vendita o mette altrimenti in circolazione, al fine di trarne profitto, i prodotti di cui al primo comma è punito con la reclusione fino a due anni e con la multa fino a euro 20.000. I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

1.2 Attività sensibili

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

Gestione dei contenziosi giudiziari e stragiudiziali con personale dipendente ed ex dipendente e collaboratori esterni

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, escluso l'ambito della liquidazione tecnica (cause di lavoro, vertenze tributarie, contenzioso societario, ecc.).

L'attività non è stata considerata in quanto ritenuta poco rilevante.

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)

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.

Assunzione e gestione del personale

Si tratta delle attività di selezione e assunzione di personale dipendente e 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 (ad esempio, Guardia di Finanza, Agenzia delle Entrate), 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.

L'attività non è stata considerata in quanto ritenuta poco rilevante.

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

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

Segregazione delle attività/funzioni/processo

Si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza 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 della società. In particolare l'assunzione del personale non deve prescindere da quanto di seguito indicato:

- criteri di selezione dei candidati oggettivi e trasparenti (ad esempio, voto di laurea/diploma, conoscenza di lingue straniere, precedenti esperienze professionali, ecc.);
- tracciabilità delle fonti di reperimento dei curricula (ad esempio, inserzioni, domande spontanee, segnalazioni interne, società di head-hunting, ecc.);
- 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;
- segregazione delle funzioni coinvolte nel processo di richiesta di assunzione di personale e in quello di valutazione/selezione o promozione del personale stesso;
- definizione di ruoli e responsabilità dei soggetti coinvolti;
- modalità di archiviazione della documentazione rilevante.

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 dei 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.

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

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 sono descritti di seguito.

False comunicazioni sociali (Art. 2621 c.c.)

Salvo quanto previsto dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta. Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

False comunicazioni sociali in danno della società, dei soci o dei creditori (Art. 2622 c.c.)

- 1. Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionano un danno patrimoniale alla società, ai soci o ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
- 2. 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.*
- 3. Nel caso di società soggette alle disposizioni della parte IV, titolo III, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è procedibile d'ufficio.*
- 4. La pena è da due a sei anni se, nelle ipotesi di cui al terzo comma, il fatto cagiona un grave nocumento ai risparmiatori.*
- 5. 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 riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo.*
- 6. La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.*
- 7. La punibilità per i fatti previsti dal primo e terzo comma è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale*

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

8. *In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.*
9. *Nei casi previsti dai commi settimo e ottavo, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.*

Falso in prospetto (Art. 173-bis TUF)

Chiunque, allo scopo di conseguire per sé o per altri un ingiusto profitto, 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, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto, espone false informazioni od occulta dati o notizie in modo idoneo ad indurre in errore i suddetti destinatari è punito, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino ad un anno. Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari del prospetto, la pena è dalla reclusione da uno a tre anni.

Falsità nelle relazioni o nelle comunicazioni delle società di revisione (Art. 27 D. Lgs 39/2010)

I responsabili della revisione i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione, sono puniti, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino a un anno. Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari delle comunicazioni, la pena è della reclusione da uno a quattro anni.

Impedito controllo (Art. 2625 c.c.)

Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione, sono puniti con la sanzione amministrativa

pecuniaria fino a 10.329 euro. Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

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

Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno.

Illegali ripartizione degli utili e delle riserve (Art. 2627 c.c.)

Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

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

Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge. Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

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

Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo

unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, della legge 12 agosto 1982, n. 576, o del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.

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

Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno.

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

I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni.

Aggiotaggio (Art. 2637 c.c.)

Chiunque diffonde notizie false, ovvero pone 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 che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni.

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

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro

anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

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 riguardano 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 dell'ente richiesto da disposizioni di legge e dell'attività e degli adempimenti legislativi legati alla tenuta dei registri contabili 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.

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

I controlli generali relativi alle attività in oggetto sono descritti 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 nelle 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.

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.)

Tracciabilità

Si richiede l'esistenza di presidi che, in relazione ad ogni comunicazione scritta, assicurino 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, il Collegio Sindacale 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 l'Organismo di Vigilanza

L'Organismo di Vigilanza deve ricevere copia delle richieste ufficiali di informazioni o documentazione provenienti dai soci, da Collegio Sindacale o dalla società di revisione.

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.

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.

Comunicazione del conflitto di interesse

L'Amministratore deve dare notizia agli altri Amministratori e al Collegio Sindacale di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata; se si tratta di amministratore delegato, deve altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale, se si tratta di amministratore unico, deve darne notizia anche alla prima assemblea utile, ai sensi dell'art. 2391 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, assicurino 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/collaboratori esterni;
- 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:

- a) attività di gestione dei flussi finanziari che definisca, fra l'altro:
 - ruoli e responsabilità dei soggetti coinvolti;

- pianificazione, da parte delle funzioni aziendali, del proprio fabbisogno finanziario e comunicazione dello stesso alla funzione Amministrazione e Finanza;
 - tipologie di transazioni eseguibili direttamente dalle varie funzioni aziendali;
 - controlli specifici e preventivi da applicarsi in casi, tassativamente previsti, in deroga alla normale procedura (es. pagamenti urgenti);
 - regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e discrezionalità;
 - controllo della correttezza dei flussi finanziari aziendali con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo;
- b) selezione e valutazione dei consulenti/collaboratori esterni con previsione, fra l'altro, di quanto di seguito indicato:
- 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.);
 - competitive bidding fra più consulenti;
 - separazione di funzioni tra coloro che selezionano e coloro che ne controllano l'operato;
 - modalità di gestione delle eccezioni alla procedura standard (ad esempio, acquisti di consulenze senza competitive bidding e/o in situazioni di emergenza);
- c) gestione degli omaggi e iniziative promozionali con previsione, fra l'altro, di quanto di seguito indicato:
- definizione di ruoli/responsabilità dei soggetti coinvolti;
 - definizione delle categorie dei possibili beneficiari degli omaggi, iniziative promozionali e apparecchiature in comodato;
 - indicazione di limiti di valore degli omaggi e delle apparecchiature concesse in comodato, nonché di limiti di durata dei contratti di comodato;
 - definizione di importi massimi e specifiche autorizzazioni per le spese di viaggio di clienti e potenziali clienti;
 - tracciabilità del processo decisionale e delle relative motivazioni;
 - 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.

Quadratura e Riscontri

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

Gestione omaggi e utilità

Al personale dipendente è fatto divieto di offrire o ricevere da rappresentanti ed esponenti della Pubblica Amministrazione regali, denaro, omaggi a vario titolo, procacciare affari e/o impieghi.

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.

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 in oggetto.

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

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 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.

Decreto legislativo 24 febbraio 1998, n. 58 “Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52” Parte V – Sanzioni Titolo I–bis – Abuso di informazioni privilegiate e manipolazione del mercato Capo II – Sanzioni penali

Informazione privilegiata (Art. 181)

1. Ai fini del presente titolo per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.
2. In relazione ai derivati su merci, per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più derivati su merci, che i partecipanti ai mercati su cui tali derivati sono negoziati si aspettano di ricevere secondo prassi di mercato ammesse in tali mercati.
3. Un'informazione si ritiene di carattere preciso se:
 - a) si riferisce ad un complesso di circostanze esistente o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà;
 - b) è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento di cui alla lettera a) sui prezzi degli strumenti finanziari.
4. Per informazione che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di strumenti finanziari si intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.

5. Nel caso delle persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

Abuso di informazioni privilegiate (art. 184 TUF)

1. E' punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro tre milioni 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. La stessa pena di cui al comma 1 si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al medesimo comma 1.
3. Il giudice può aumentare la 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.
4. Ai fini del presente articolo per strumenti finanziari si intendono anche gli strumenti finanziari di cui all'articolo 1, comma 2, il cui valore dipende da uno strumento finanziario di cui all'art. 180¹⁵, comma 1, lettera a).

¹⁵Ai fini del presente titolo si intendono per:

a) "strumenti finanziari":

1) gli strumenti finanziari di cui all'articolo 1, comma 2 [dell'Art.180 del TUF, "Definizioni"], ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione europea, nonché qualsiasi altro strumento ammesso o per il quale è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato di un Paese dell'Unione europea;

2) gli strumenti finanziari di cui all'articolo 1, comma 2, ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano, per i quali l'ammissione è stata richiesta o autorizzata dall'emittente.

Manipolazione del mercato (art. 185 TUF)

1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni.
2. Il giudice può aumentare la 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.

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

1. Salve le sanzioni penali quando il fatto costituisce reato, è punito con la sanzione amministrativa pecuniaria da euro ventimila a euro tre milioni 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:
 2. 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;
 3. b) comunica informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
 4. c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).
5. La stessa sanzione di cui al comma 1 si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni di cui al medesimo comma 1.
6. Ai fini del presente articolo per strumenti finanziari si intendono anche gli strumenti finanziari di cui all'art. 1, comma 2, il cui valore dipende da uno strumento finanziario di cui all'art. 180, comma 1, lettera a).
7. La sanzione prevista al comma 1 si applica anche a chiunque, in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse, compie taluno dei fatti ivi descritti.
8. Le sanzioni amministrative pecuniarie previste dai commi 1, 2 e 4 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.

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

Manipolazione del mercato (art. 187-ter TUF)

1. Salve le sanzioni penali quando il fatto costituisce reato, è punito con la sanzione amministrativa pecuniaria da euro ventimila a euro cinque milioni 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.
2. 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.
3. Salve le sanzioni penali quando il fatto costituisce reato, è punito con la sanzione amministrativa pecuniaria di cui al comma 1 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.
4. Per gli illeciti indicati al comma 3, 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.
5. 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.

6. Il Ministero dell'economia e delle finanze, sentita la CONSOB ovvero su proposta della medesima, può individuare, con proprio regolamento, in conformità alle disposizioni di attuazione della direttiva 2003/6/CE adottate dalla Commissione europea, secondo la procedura di cui all'articolo 17, paragrafo 2, della stessa direttiva, le fattispecie, anche ulteriori rispetto a quelle previste nei commi precedenti, rilevanti ai fini dell'applicazione del presente articolo.
7. La CONSOB rende noti, con proprie disposizioni, gli elementi e le circostanze da prendere in considerazione per la valutazione dei comportamenti idonei a costituire manipolazioni di mercato, ai sensi della direttiva 2003/6/CE e delle disposizioni di attuazione della stessa.

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

Gestione delle informazioni che si possono definire privilegiate ai sensi dell'articolo 181 TUF.

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 relativi alle attività in oggetto sono descritti di seguito.

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

Con riferimento a tale attività sensibile, 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 per la comunicazione 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.

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.

Autorizzazione formale

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.

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.

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.

5. 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.

Pur nella consapevolezza che la normativa qui richiamata (D.Lgs. 231/07 e seguenti) non si applica direttamente ad Aviva Italia Holding S.p.A. in quanto la Compagnia esercita esclusivamente i rami danni, si è comunque ritenuto opportuno illustrare l'area di rischio connessa ai reati di ricettazione, riciclaggio e impiego di denaro, di beni o di utilità di provenienza illecita ed i relativi presidi di controllo.

Tale scelta è giustificata dal fatto che la Compagnia appartiene ad un Gruppo assicurativo del quale fanno parte anche Compagnie che esercitano i rami vita e che le Compagnie sono tra loro collegate da rapporti di fornitura di servizi.

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

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, 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 transnazionalità:

Ricettazione (art. 648 c.p.)

Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329. La pena è della reclusione sino a sei anni e della multa sino a

euro 516, se il fatto è di particolare tenuità. Le disposizioni di questo articolo si applicano 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.)

Fuori dei casi di concorso nel reato, chiunque 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, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.

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

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648–bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a 15.493. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648. Si applica l'ultimo comma dell'articolo 648.

5.2 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:

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

Selezione fornitori, pagamento corrispettivi contrattuali, attività di investimento con il patrimonio libero, attività inerenti alla gestione dei flussi finanziari

5.3 Sistema dei controlli

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;

5.3.1 Controlli generali

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

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

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

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

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

Verifiche preventive

Deve essere svolta, con particolare riferimento ai fornitori di beni e servizi di importo rilevante, 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).

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, 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.

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.

6. 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.

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

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, 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.

6.2. 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

Esecuzione delle istruzioni, e conseguenti procedure interne, in materia di contrasto finanziario del terrorismo da chiunque emanate (Istituzioni europee, Organismi nazionali, UIF, ecc.).

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

Adempimenti legati alla gestione delle iniziative umanitarie e di solidarietà terrorismo (ad es. identificazione beneficiari donazioni o liberalità).

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.

6.3 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.

6.3.1 Controlli generali

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

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

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.

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, 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.

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.

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.

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

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.)

Chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento, è punito con la reclusione da otto a venti anni. La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittare di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona. La pena è aumentata da un terzo alla metà se i fatti di cui al primo comma sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

Prostituzione minorile (Art. 600–bis c.p.)

Chiunque induce alla prostituzione una persona di età inferiore agli anni diciotto ovvero ne favorisce o sfrutta la prostituzione è punito con la reclusione da sei a dodici anni e con la multa da euro 15.493 a euro 154.937. Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di denaro o di altra utilità economica, è punito con la reclusione da sei mesi a tre anni e con la multa non inferiore a euro 5.164. Nel caso in cui il fatto di cui al secondo comma sia commesso nei confronti di persona che non abbia compiuto gli anni sedici, si applica la pena della reclusione da due a

cinque anni. Se l'autore del fatto di cui al secondo comma è persona minore di anni diciotto si applica la pena della reclusione o della multa, ridotta da un terzo a due terzi.

Pornografia minorile (Art. 600-ter c.p.)

Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche è punito con la reclusione da sei a dodici anni e con la multa da euro 25.822 a euro 258.228. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164. Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità.

Detenzione di materiale pornografico (Art. 600-quater c.p.)

Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.

Pornografia virtuale (Art. 600-quater.1 c.p.)

Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Iniziativa turistiche volte allo sfruttamento della prostituzione minorile (Art. 600-quinquies c.p.)

Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da euro 15.493 e euro 154.937.

Tratta di persone (Art. 601 c.p.)

Chiunque commette tratta di persona che si trova nelle condizioni di cui all'articolo 600 ovvero, al fine di commettere i delitti di cui al primo comma del medesimo articolo, la induce mediante

inganno o la costringe mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno, è punito con la reclusione da otto a venti anni. La pena è aumentata da un terzo alla metà se i delitti di cui al presente articolo sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

Acquisto e alienazione di schiavi (Art. 602 c.p.)

Chiunque, fuori dei casi indicati nell'articolo 601, acquista o aliena o cede una persona che si trova in una delle condizioni di cui all'articolo 600 è punito con la reclusione da otto a venti anni. La pena è aumentata da un terzo alla metà se la persona offesa è minore degli anni diciotto ovvero se i fatti di cui al primo comma sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

Pratiche di mutilazione degli organi genitali femminili (Art. 583–bis c.p.)

Chiunque, in assenza di esigenze terapeutiche, cagiona una mutilazione degli organi genitali femminili è punito con la reclusione da quattro a dodici anni. Ai fini del presente articolo, si intendono come pratiche di mutilazione degli organi genitali femminili la clitoridectomia, l'escissione e l'infibulazione e qualsiasi altra pratica che cagioni effetti dello stesso tipo. Chiunque, in assenza di esigenze terapeutiche, provoca, al fine di menomare le funzioni sessuali, lesioni agli organi genitali femminili diverse da quelle indicate al primo comma, da cui derivi una malattia nel corpo o nella mente, è punito con la reclusione da tre a sette anni. La pena è diminuita fino a due terzi se la lesione è di lieve entità. La pena è aumentata di un terzo quando le pratiche di cui al primo e al secondo comma sono commesse a danno di un minore ovvero se il fatto è commesso per fini di lucro. Le disposizioni del presente articolo si applicano altresì quando il fatto è commesso all'estero da cittadino italiano o da straniero residente in Italia, ovvero in danno di cittadino italiano o di straniero residente in Italia. In tal caso, il colpevole è punito a richiesta del Ministro della giustizia.

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"

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

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

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.

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 relativi alle attività in oggetto sono descritti di seguito.

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 all'impegno a tutelare le personalità individuali.

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 principi relativi all'impegno a tutelare le personalità individuali.

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 principi relativi all'impegno a tutelare le personalità individuali.

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 principi relativi all'impegno a tutelare le personalità individuali.

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.

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.

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

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, ai sensi del D.Lgs. 9 aprile 2008, n. 81.

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.

Dall'analisi normativa svolta, i principali reati risultano essere i seguenti:

Omicidio colposo (Art. 589 c.p.)

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni. Si applica la pena della reclusione da tre a dieci anni se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale da: 1) soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni; 2) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

Lesioni personali colpose (Art. 590 c.p.)

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309. Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239. Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto è commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni. Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque. Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

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:

Gestione sicurezza e igiene sul lavoro (D.Lgs. 81/08)

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 Responsabile del Servizio di Prevenzione e Protezione (RSPP);
- creazione e gestione di un Servizio di Prevenzione e Protezione (SPP);
- nomina di preposti Addetti al Servizio di Prevenzione e Protezione (ASPP) 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. 26 del D.Lgs. 81/08 (così come modificato dalla Legge 123/07, art. 7) 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 relativi alle attività in oggetto sono descritti di seguito.

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,, Rappresentanti dei Lavoratori per la Sicurezza ("RLS"), Addetti al servizio di Protezione e Prevenzione ("APP"), Responsabili del Servizio di Prevenzione e Protezione ("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.

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.

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.

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

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 c.p.)

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

Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse

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

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

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617–quater.

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

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

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

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617–quinquies c.p.)

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

Danneggiamento di informazioni, dati e programmi informatici (Art. 635–bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635¹⁶ ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635–ter c.p.)

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

Danneggiamento di sistemi informatici o telematici (Art. 635–quater c.p.)

¹⁶ Danneggiamento (Art. 635 c.p.)

Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa con la reclusione fino a un anno o con la multa fino a lire seicentomila.

La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso:

- 1) con violenza alla persona o con minaccia;
- 2) da datori di lavoro in occasione di serrate, o da lavoratori in occasione di sciopero, ovvero in occasione di alcuno dei delitti preveduti dagli artt. 330, 331 e 333¹⁶;
- 3) su edifici pubblici o destinati a uso pubblico all'esercizio di un culto, o su altre delle cose indicate nel n. 7 dell'articolo 625;
- 4) sopra opere destinate all'irrigazione;
- 5) sopra piante di viti, di alberi o arbusti fruttiferi, o su boschi, selve o foreste, ovvero su vivai forestali destinati al rimboschimento.

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

Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.)

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

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640-quinquies c.p.)

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

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 relativi alle attività in oggetto sono descritti di seguito.

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 delle 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 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.).

Gestione 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 causa comune agli incidenti;
- 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 rimedi 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 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.

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.

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.

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

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) – Articolo aggiunto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29

Associazione per delinquere (Art. 416 c.p.)

Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. I capi soggiacciono alla stessa pena stabilita per i promotori. Se

gli associati scendono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più. Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.

Associazione di tipo mafioso (Art. 416-bis c.p.)

Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da tre a sei anni. Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da quattro a nove anni. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali. Se l'associazione è armata si applica la pena della reclusione da quattro a dieci anni nei casi previsti dal primo comma e da cinque a quindici anni nei casi previsti dal secondo comma. L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplosive, anche se occultate o tenute in luogo di deposito. Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà. Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego. Le disposizioni del presente articolo si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

Scambio elettorale politico-mafioso (Art. 416-ter c.p.)

La pena stabilita dal primo comma dell'articolo 416bis si applica anche a chi ottiene la promessa di voti prevista dal terzo comma del medesimo articolo 416bis in cambio della erogazione di denaro

Sequestro di persona a scopo di rapina o di estorsione (Art. 630 c.p.)

Chiunque sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione, è punito con la reclusione da venticinque a trenta anni. Se dal sequestro deriva comunque la morte, quale conseguenza non voluta dal reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta. Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo. Al concorrente che, dissociandosi dagli altri, si adopera in modo che il soggetto passivo riacquisti la libertà, senza che tale risultato sia conseguenza del prezzo della liberazione, si applicano le pene previste dall'articolo 605. Se tuttavia il soggetto passivo muore, in conseguenza del sequestro, dopo la liberazione, la pena è della reclusione da sei a quindici anni. Nei confronti del concorrente che, dissociandosi dagli altri, si adopera, al di fuori del caso previsto dal comma precedente, per evitare che l'attività delittuosa sia portata a conseguenze ulteriori ovvero aiuta concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di prove decisive per l'individuazione o la cattura dei concorrenti, la pena dell'ergastolo è sostituita da quella della reclusione da dodici a venti anni e le altre pene sono diminuite da un terzo a due terzi. Quando ricorre una circostanza attenuante, alla pena prevista dal secondo comma è sostituita la reclusione da venti a ventiquattro anni; alla pena prevista dal terzo comma è sostituita la reclusione da ventiquattro a trenta anni. Se concorrono più circostanze attenuanti, la pena da applicare per effetto delle diminuzioni non può essere inferiore a dieci anni, nell'ipotesi prevista dal secondo comma, ed a quindici anni, nell'ipotesi prevista dal terzo comma. I limiti di pena preveduti nel comma precedente possono essere superati allorché ricorrono le circostanze attenuanti di cui al quinto comma del presente articolo.

Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (Art. 74, DPR 309/90)

Quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 73, chi promuove, costituisce, dirige, organizza o finanzia l'associazione è punito per ciò solo con la reclusione non inferiore a venti anni. Chi partecipa all'associazione è punito con la reclusione non inferiore a dieci anni. La pena è aumentata se il numero degli associati è di dieci o più o se tra i partecipanti vi sono persone dedite all'uso di sostanze stupefacenti o psicotrope. Se l'associazione è armata la pena, nei casi indicati dai commi 1 e 3, non può essere inferiore a ventiquattro anni di reclusione e, nel caso previsto dal comma 2, a dodici anni di reclusione. L'associazione si considera armata quando i partecipanti hanno la disponibilità di armi o materie esplosive, anche se occultate o tenute in luogo di deposito. La pena è aumentata se ricorre la circostanza di cui alla lettera e) del comma 1 dell'articolo 80. Se l'associazione è costituita per commettere i fatti descritti dal comma 5 dell'articolo 73, si applicano il primo e il secondo comma dell'articolo 416 del codice penale. Le pene previste dai commi da 1 a 6 sono diminuite dalla metà a due terzi per chi si sia efficacemente adoperato per assicurare le prove del reato o per

sottrarre all'associazione risorse decisive per la commissione dei delitti. Quando in leggi e decreti è richiamato il reato previsto dall'articolo 75 della legge 22 dicembre 1975, n. 685, abrogato dall'articolo 38, comma 1, della legge 26 giugno 1990, n. 162, il richiamo si intende riferito al presente articolo.

Art. 407, co. 2, lett. a), n. 5), c.p.p.

Delitti di 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 previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110¹⁷.

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.)

Chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio è punito, a querela della persona offesa, se il fatto non costituisce un più grave reato, con la reclusione fino a due anni e con la multa da centotré euro a milletrentadue euro.

Illecita concorrenza con minaccia o violenza (Art. 513-bis c.p.)

Chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia è punito con la reclusione da due a sei anni. La pena è aumentata se gli atti di concorrenza riguardano un'attività finanziata in tutto o in parte ed in qualsiasi modo dallo Stato o da altri enti pubblici.

Frodi contro le industrie nazionali (Art. 514 c.p.)

Chiunque, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagiona un nocumento all'industria nazionale, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a cinquecentosedici euro. Se per i marchi o segni distintivi sono state osservate le norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà industriale, la pena è aumentata e non si applicano le disposizioni degli articoli 473 e 474.

Frode nell'esercizio del commercio (Art. 515 c.p.)

¹⁷ Sono infine considerate armi comuni da sparo 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 di cui all'articolo 6 escluda, in relazione alle rispettive caratteristiche, l'attitudine a recare offesa alla persona.

Chiunque, nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita, è punito, qualora il fatto non costituisca un più grave delitto, con la reclusione fino a due anni o con la multa fino a duemilasesantacinque euro. Se si tratta di oggetti preziosi, la pena è della reclusione fino a tre anni o della multa non inferiore a centotre euro.

Vendita di sostanze alimentari non genuine come genuine (Art. 516 c.p.)

Chiunque pone in vendita o mette altrimenti in commercio come genuine sostanze alimentari non genuine è punito con la reclusione fino a sei mesi o con la multa fino a milletrentadue euro.

Vendita di prodotti industriali con segni mendaci (Art. 517 c.p.)

Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa fino a milletrentadue euro.

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (Art. 517-ter c.p.)

Salva l'applicazione degli articoli 473 e 474 chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso è punito, a querela della persona offesa, con la reclusione fino a due anni e con la multa fino a euro 20.000. Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al primo comma. Si applicano le disposizioni di cui agli articoli 474-bis, 474-ter, secondo comma, e 517-bis, secondo comma. I delitti previsti dai commi primo e secondo sono punibili sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (Art. 517-quater c.p.)

Chiunque contraffà o comunque altera indicazioni geografiche o denominazioni di origine di prodotti agroalimentari è punito con la reclusione fino a due anni e con la multa fino a 20.000 euro. Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i medesimi prodotti con le indicazioni o denominazioni contraffatte. Si applicano le disposizioni di cui agli articoli 474-bis, 474-ter, secondo comma, e 517-bis, secondo comma. I

delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali in materia di tutela delle indicazioni geografiche e delle denominazioni di origine dei prodotti agroalimentari.

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

Art. 171 Legge 22 aprile 1941, n. 633

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 Legge 22 aprile 1941, n. 633

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–quinqüies 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 Legge 22 aprile 1941, n. 633

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-^{ter} 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 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 Legge 22 aprile 1941, n. 633

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 Legge 22 aprile 1941, n. 633

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.

Art. 181–bis, comma 2, Legge 22 aprile 1941, n. 633

Il contrassegno è apposto sui supporti di cui al comma 1 ai soli fini della tutela dei diritti relativi alle opere dell'ingegno, previa attestazione da parte del richiedente dell'assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi. In presenza di seri indizi, la SIAE verifica, anche successivamente, circostanze ed elementi rilevanti ai fini dell'apposizione Comma 1 (estratto): "ogni supporto contenente programmi per elaboratore o multimediali nonché su ogni supporto contenente suoni, voci o immagini in movimento, che reca la fissazione di opere o di parti di opere tra quelle indicate nell'articolo 1, primo comma, destinati ad essere posti comunque in commercio o ceduti in uso a qualunque titolo a fine di lucro".

Art. 1, comma 1, Legge 22 aprile 1941, n. 633

Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione.

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.)

Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni.

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.

L'attività in oggetto non è applicabile al contesto di riferimento.

Produzione e commercio di prodotti

Fabbricazione e commercio di prodotti industriali e agroalimentari.

L'attività in oggetto non è applicabile al contesto di riferimento.

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

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

Segregazione delle attività/funzioni/processo

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

Gestione documenti tutelati dal diritto d'autore

Autorizzazione formale

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

Gestione rapporti con autorità giudiziaria

Autorizzazione formale

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

Registrazione

L'operazione deve essere registrata e documentata 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.

Gruppo Aviva

V.le Abruzzi 94 - 20131 Milano

www.avivaitalia.it

Tel. +39 02 2775.1

Fax +39 02 2775.204

