

**PARTE SPECIALE**

1.	ARTICOLAZIONE DEI POTERI E SISTEMA DELLE DELEGHE .....	4
1.1.	Principi ispiratori del sistema di articolazione dei poteri delle deleghe .....	4
1.2.	Il sistema dei poteri e delle deleghe .....	4
2.	FINALITA' DELLA PARTE SPECIALE .....	5
2.1.	Struttura della parte speciale .....	5
2.2.	Specifiche circa i delitti tentati .....	6
3.	– SEZIONE “A” – REATI CONTRO LA PUBBLICA AMMINISTRAZIONE .....	7
3.1.	Introduzione e funzione della parte speciale dedicata ai reati contro la Pubblica Amministrazione .....	7
3.2.	Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di un pubblico servizio .....	7
3.3.	Le fattispecie di reato richiamate dal D.Lgs 231/01 .....	9
3.3.1.	Malversazione a danno dello Stato o dell’Unione Europea (Art. 316 bis c.p.) .....	10
3.3.2.	Indebita percezione di erogazioni a danno dello Stato (Art. 316 ter c.p.) .....	10
3.3.3.	Truffa in danno dello Stato o di altro Ente Pubblico o dell’Unione Europea (Art. 640 – Comma 2, numero 1, c.p.) .....	10
3.3.4.	Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640 bis c.p.) .....	10
3.3.5.	Frode informatica in danno dello Stato o di altro Ente Pubblico (Art. 640 ter c.p.) .....	11
3.3.6.	Corruzione in atti giudiziari (Art. 319-ter c.p.) .....	11
3.3.7.	Istigazione alla corruzione (Art. 322 c.p.) .....	11
3.4.	Le attività sensibili relative ai reati contro la Pubblica Amministrazione .....	11
3.5.	Organi e funzioni aziendali coinvolte .....	12
3.6.	Principi e regole di comportamento .....	13
3.7.	Principi e norme generali di comportamento .....	15
3.8.	Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili .....	16
3.9.	I controlli dell’Organismo di Vigilanza .....	17
4.	– SEZIONE “B” – REATI SOCIETARI .....	19
4.1.	Introduzione e funzione della parte speciale dedicata ai reati societari .....	19
4.2.	Le fattispecie di reato richiamate dal D.Lgs 231/01 .....	19
4.2.1.	False comunicazioni sociali (Artt. 2621 e 2622 c.c.) .....	19
4.2.2.	Falso in prospetto (art. 173-bis D.Lgs. n. 58 del 1998 aggiornato con D.lgs. n. 164 del 17.09.2007) .....	19
4.2.3.	Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.) .....	20
4.2.4.	Impedito controllo (art. 2625 c.c.) .....	20
4.2.5.	Formazione fittizia del capitale (art. 2632 c.c.) .....	20
4.2.6.	Indebita restituzione dei conferimenti (art. 2626 c.c.) .....	20
4.2.7.	Illegale ripartizioni degli utili o delle riserve (art. 2627 c.c.) .....	21
4.2.8.	Illecite operazioni sulle azioni o quote sociali o delle società controllate (art. 2628 c.c.) .....	21
4.2.9.	Operazioni in pregiudizio dei creditori (art. 2629 c.c.) .....	21
4.2.10.	Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.) .....	21
4.2.11.	Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.) .....	21

**PARTE SPECIALE**

4.2.12.	Illecita influenza sull'assemblea (art. 2636 c.c.).....	22
4.2.13.	Corruzione tra privati (art. 2635 c.c.).....	22
4.3.	Le attività sensibili relative ai reati societari.....	22
4.4.	Organi e funzioni aziendali coinvolte.....	23
4.5.	Principi e regole di comportamento.....	23
4.6.	Principi e norme generali di comportamento.....	24
4.7.	Principi di riferimento speciali relativi alla regolamentazione delle attività sensibili.....	24
4.8.	I controlli dell'Organismo di Vigilanza.....	28
5.	<b>– SEZIONE “C” – REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE COMMESSE CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICA.....</b>	<b>29</b>
5.1.	Introduzione e funzione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antifortunistica.....	29
5.2.	Criteri per la definizione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antifortunistiche.....	30
5.3.	Le fattispecie di reato richiamate dal D.Lgs 231/01.....	30
5.3.1.	Omicidio Colposo (art. 589 c.p.).....	30
5.3.2.	Lesioni personali colpose gravi e gravissime (art. 589 c.p.).....	31
5.4.	Le Sanzioni previste dal Decreto.....	32
5.5.	Le attività sensibili relative ai reati di omicidio colposo e lesioni colpose commesse.....	32
5.6.	Organi e funzioni aziendali coinvolte.....	33
5.7.	Principi e norme generali di comportamento.....	33
5.8.	Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili.....	35
5.9.	Attività di Informazione e Formazione.....	41
5.10.	Istituzione di flussi informativi.....	42
5.11.	Conservazione della documentazione rilevante.....	42
5.12.	Contratto d'appalto.....	43
5.13.	I Controlli dell'Organismo di Vigilanza.....	44
6.	<b>– SEZIONE “D” – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI.....</b>	<b>45</b>
6.1.	Introduzione e funzione della parte speciale dei reati informatici e di trattamento illecito dei dati.....	45
6.2.	Criteri per la definizione dei reati informatici e di trattamento illecito dei dati.....	45
6.3.	Le fattispecie di reato richiamate dal D.Lgs 231/01.....	45
6.3.1.	Falsità in documenti informatici (art. 491-bis c.p.).....	45
6.3.2.	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.).....	45
6.3.3.	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).....	46
6.4.	Le attività sensibili relative ai reati informatici.....	46
6.5.	Organi e funzioni aziendali coinvolte.....	47
6.6.	Principi e regole di comportamento.....	47
6.7.	Principi e norme generali di comportamento.....	47
6.8.	Principi di riferimento e specifici relativi alla regolamentazione delle attività sensibili.....	48

**PARTE SPECIALE**

6.9.	I controlli dell'Organismo di Vigilanza .....	51
7.	– SEZIONE “E” – REATI AMBIENTALI .....	52
7.1.	Introduzione e funzione della parte speciale dei reati ambientali.....	52
7.2.	Criteri per la definizione dei reati ambientali .....	52
7.3.	Le fattispecie di reato richiamate dal D.Lgs 231/01 .....	52
7.3.1.	Scarichi di acque reflue (art. 137, D.Lgs 152/2006) .....	52
7.3.2.	Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, D.Lgs 152/2006) 53	
7.3.3.	Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, D.Lgs 152/2006).....	54
7.3.4.	Superamento valori limite di emissione (art. 279, D.Lgs 152/2006) .....	54
7.3.5.	Falsificazione o alterazione di certificati e licenze (art. 3-bis, Legge 150/1992) .....	55
7.3.6.	Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3-bis, Legge 150/1992).....	55
7.4.	Le attività sensibili relative ai reati ambientali .....	56
7.5.	Organi e funzioni aziendali coinvolte.....	56
7.6.	Principi e regole di comportamento .....	57
7.7.	Principi e norme generali di comportamento .....	57
7.8.	Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili .....	58
7.9.	Impegni per la salvaguardia ambientale.....	59
7.10.	Controlli dell'Organismo di Vigilanza.....	60

## **1. ARTICOLAZIONE DEI POTERI E SISTEMA DELLE DELEGHE**

### **1.1. Principi ispiratori del sistema di articolazione dei poteri delle deleghe**

Il sistema adottato delle deleghe e dei poteri costituisce parte integrante e sostanziale del Modello 231 aziendale.

Il principio cui l'azienda ispira la propria struttura organizzativa e la propria attività è quello in base al quale solo i soggetti muniti di specifici e formali poteri possono assumere, in suo nome e per suo conto, obbligazioni verso terzi.

I principi ispiratori di tale sistema sono:

- La tempestiva e costante informazione circa la titolarità dei poteri delegati ed i relativi cambiamenti;
- La verifica periodica del rispetto dei poteri così come delegati;
- Le dichiarazioni periodiche di cui sia determinata nel Modello 231 la cadenza con le quali coloro che hanno ricevuto deleghe di poteri confermino il rispetto degli stessi nonché dei principi del codice etico e l'assenza di conflitti di interesse;
- La verifica periodica dell'adeguatezza del sistema delle deleghe.

A tutti i poteri attribuiti mediante delega degli stessi corrispondono esattamente mansioni e responsabilità come riportate nell'organigramma dell'Azienda.

Il sistema dei poteri e delle deleghe prevede che:

- Ogni destinatario del presente Modello 231 che, per conto dell'Azienda intrattiene rapporti negoziali e/o di rappresentanza con l'esterno, deve essere dotato di idonea procura;
- Tutti coloro (ivi compreso anche i dipendenti o gli organi sociali) che intrattengono per conto dell'Azienda rapporti con la Pubblica Amministrazione, devono essere dotati di delega formale in tal senso;
- Ciascuna delega definisce in dettaglio i poteri del delegato e del soggetto.

L'Organismo di Vigilanza verifica periodicamente il sistema delle deleghe e delle procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche.

Il conferimento della procura è seguito da una lettera di accompagnamento da trasmettere al procuratore unitamente all'atto di conferimento della procura e contenente il richiamo al Modello 231, alle disposizioni del Codice Etico ed alle procedure operative interne.

### **1.2. Il sistema dei poteri e delle deleghe**

Il principio della segregazione delle responsabilità è applicato in azienda in linea con quanto consentito dalla normativa vigente.

I poteri di firma e di rappresentanza sono rilasciati dal legale rappresentante aziendale e sono revocabili in qualsiasi momento attraverso una semplice notifica a seguito della decisione della società.

Il sistema dei poteri e delle deleghe prevede l'attribuzione dei poteri di rappresentanza sia alla Direzione aziendale sia ad ulteriori procuratori (come consulenti esterni, dipendenti, etc.).

I poteri rappresentativi (sia degli amministratori che dei procuratori) sono distinti in formali ed operativi. Mentre i poteri elencati sono indistintamente attribuiti a ciascun amministratore, le deleghe dei procuratori sono conferite in funzione delle attività svolte da ciascuno.

Nell'Azienda le procure si dividono in:

- operative, per atti di gestione ordinaria
- di rappresentanza
- di responsabilità

Per determinare categorie di atti che prevedano un impegno ultra annuale o che superino uno specifico importo, è prevista l'autorizzazione della Direzione aziendale fatti salvi i casi di urgenza specificatamente approvati.

## **2. FINALITA' DELLA PARTE SPECIALE**

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello 231 dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nella Società, la commissione di reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale del Modello 231 ha lo scopo di:

- Indicare le modalità che gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'OdV ed alle altre funzioni di controlli gli strumenti per esercitare le attività di monitoraggio, controllo e verifica;

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi ai contenuti dei seguenti documenti:

- Modello 231
- Codice Etico
- Procedure e disposizioni
- Procure e deleghe
- Ordini di servizio
- Comunicazioni organizzative
- Sistemi di gestione delle problematiche di salute e sicurezza e ambientali
- Ogni altro documenti che regoli attività rientranti nell'ambito di applicazione del Decreto

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

### **2.1. Struttura della parte speciale**

La presente Parte Speciale è composta da una parte preliminare dedicata alle regole generali cui si uniforma la condotta degli organi sociali, dei dipendenti, dei partner commerciali, dei collaboratori o consulenti e dei soggetti esterni che operano in nome e per conto dell'Azienda (qui di seguito, per brevità, semplicemente "destinatari del Modello 231" ed all'individuazione delle aree di attività a rischio, nonché da singole sezioni dedicate alle categorie di reati presi in considerazione dal Decreto e considerate sensibili dalla società a seguito di gap-analysis.

Le sezioni della Parte Speciale sono le seguenti:

<b>SEZIONE "A"</b>	Reati contro la Pubblica Amministrazione
<b>SEZIONE "B"</b>	Reati societari
<b>SEZIONE "C"</b>	Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
<b>SEZIONE "D"</b>	Delitti informatici e trattamento illecito di dati
<b>SEZIONE "E"</b>	Reati ambientali

## 2.2. Specifiche circa i delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del d.lgs. 231/2001). L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto.

Si tratta di un'ipotesi particolare del c.d. "recesso attivo", previsto dall'art. 56, comma 4, c.p..

### **3. – SEZIONE “A” – REATI CONTRO LA PUBBLICA AMMINISTRAZIONE**

#### **3.1. Introduzione e funzione della parte speciale dedicata ai reati contro la Pubblica Amministrazione**

Obiettivo della presente Parte Speciale è che tutti i destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei reati in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Dipendenti, gli Organi Sociali, i Collaboratori esterni e i Partner della Società sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

Provvede a fornire, inoltre, indicazioni riferite a ciascuna delle suddette categorie di reati, al fine di facilitare la comprensione delle attività e delle funzioni nell'ambito delle quali possono essere commessi i reati di cui al Decreto.

Il Consiglio di Amministrazione nel definire tale documento, a ulteriore conferma della volontà aziendale di operare secondo principi “etici” così come già contemplati nella propria regolamentazione interna, intende sensibilizzare tutto il personale a mantenere comportamenti corretti e idonei a prevenire la commissione di reati.

A tale scopo vengono disciplinati nel presente documento i principi e le regole di comportamento da porre alla base dell'operatività aziendale.

Tali principi e regole richiamano, focalizzandoli ai fini della prevenzione dei reati connessi al Decreto ed eventualmente integrandoli, quelli previsti nel Codice Etico / Codice di Comportamento Interno e nelle procedure aziendali interne attualmente in vigore, quali individuati nella Parte Generale del Modello.

#### **In via generale, a tutto il personale dell'Azienda:**

- È fatto obbligo di rispettare le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della Società richiamati nel Modello e nei quali il medesimo si articola;
- È fatto divieto di:
  - Porre in essere, dare causa o concorrere alla realizzazione di comportamenti che possano integrare, direttamente o indirettamente, qualsiasi fattispecie di reato disciplinata nella legislazione tempo per tempo vigente e, in particolare, i reati di cui al Decreto;
  - Violare in tutto o in parte le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della società richiamati nel Modello e nei quali il medesimo si articola.

La violazione delle norme aziendali e, in particolare, di quelle richiamate nel presente documento, comporta l'applicazione del sistema disciplinare illustrato nella Parte Generale.

I medesimi obblighi e divieti si applicano, per le attività e i comportamenti loro rispettivamente attribuiti o comunque ai quali sono tenuti nell'esercizio dell'ufficio o dell'incarico, ai componenti degli Organi Sociali della Azienda, ai Collaboratori esterni e ai Partner.

#### **3.2. Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di un pubblico servizio**

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo di quei soggetti qualificati come "soggetti attivi" nei reati rilevanti ai fini del Decreto, ovvero di quei soggetti la cui qualifica è necessaria ad integrare fattispecie criminose previste nel Decreto.

In aggiunta sono riportate anche delle indicazioni in merito alle fattispecie di reato che si possono compiere in relazione alle diverse categorie di soggetti coinvolti.

#### **Enti della Pubblica Amministrazione**

Agli effetti della legge penale, viene comunemente considerato come “Ente della pubblica amministrazione” qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

Sebbene non esista nel codice penale una definizione di pubblica amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano “tutte le attività dello Stato e degli altri enti pubblici”.

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l’art. 1, comma 2, D.Lgs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

A titolo esemplificativo, si possono indicare quali soggetti della pubblica amministrazione, i seguenti enti o categorie di enti:

Istituti e scuole di ogni ordine e grado e le istituzioni educative	=
Enti ed amministrazioni dello Stato ad ordinamento autonomo	Ministeri - Camera e Senato - Dipartimento Politiche Comunitarie - Autorità Garante della Concorrenza e del Mercato - Autorità per l’Energia Elettrica ed il Gas - Autorità per le Garanzie nelle Comunicazioni - Banca d’Italia – Consob - Autorità Garante per la protezione dei dati personali - Agenzia delle Entrate – ISVAP - COVIP
Regioni	=
Province	=
Comuni	=
Comunità montane e loro consorzi ed associazioni	=
Camere di Commercio, Industria, Artigianato ed Agricoltura e loro associazioni	=
Tutti gli enti pubblici non economici nazionali, regionali e locali	INPS – CNR – INAIL – INPDAI - ISTAT – ENASARCO – ASL - Enti e Monopoli di Stato - RAI

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose previste dal Decreto.

In particolare le figure che assumono rilevanza a tal fine sono soltanto quelle dei “Pubblici Ufficiali” e degli “Incaricati di Pubblico Servizio”.

### **Pubblici Ufficiali**

Ai sensi dell’Art. 357, primo comma, codice penale, è considerato pubblico ufficiale agli effetti della legge penale “colui il quale esercita una pubblica funzione legislativa, giudiziaria o amministrativa”.

Il secondo comma si preoccupa poi di definire la nozione di “pubblica funzione amministrativa”. Non si è compiuta invece un’analoga attività definitoria per precisare la nozione di “funzione legislativa” e “funzione giudiziaria” in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.

Pertanto, il secondo comma dell’articolo in esame precisa che, agli effetti della legge penale “è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”.

Tale ultima definizione normativa individua, innanzitutto, la delimitazione “esterna” della funzione amministrativa. Tale delimitazione è attuata mediante il ricorso a un criterio formale che fa riferimento alla natura della disciplina, per cui è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Il secondo comma dell’Art. 357 c.p. traduce poi in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di “pubblica funzione” da quella di “servizio pubblico”.

Vengono quindi pacificamente definite come “funzioni pubbliche” quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di:

- Poteri deliberativi
- Poteri autoritativi
- Poteri certificativi

Alla luce dei principi sopra enunciati, si può affermare che la categoria di soggetti più problematica è certamente quella che ricopre una “pubblica funzione amministrativa”.

Per fornire un contributo pratico alla risoluzione di eventuali “casi dubbi”, può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico amministrativo dello Stato o di enti territoriali, ma anche – sempre riferendoci ad un’attività di altro ente pubblico retta da norme pubblicistiche – tutti coloro che, in base allo statuto nonché alle deleghe che esso consenta, ne formino legittimamente la volontà e/o la portino all’esterno in forza di un potere di rappresentanza.

Esatto sembra infine affermare, in tale contesto, che non assumono la qualifica in esame altri soggetti che, sebbene di grado tutt’altro che modesto, svolgano solo mansioni preparatorie alla formazione della volontà dell’ente (e così, i segretari amministrativi, i geometri, i ragionieri e gli ingegneri, tranne che, in specifici casi e per singole incombenze, non “formino” o manifestino la volontà della pubblica amministrazione).

### **Incaricati di un pubblico servizio**

La definizione della categoria di “soggetti incaricati di un pubblico servizio” si rinviene all’art. 358 c. p. il quale recita che “sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio”.

Per pubblico servizio deve intendersi “ un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il “servizio”, affinché possa definirsi pubblico, deve essere disciplinato – del pari alla “pubblica funzione” - da norme di diritto pubblico ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Il legislatore ha inoltre precisato che non può mai costituire “servizio pubblico” lo svolgimento di “semplici mansioni di ordine” né la “prestazione di opera meramente materiale”. Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che ai fini della definizione come pubblico servizio dell’intera attività svolta nell’ambito di tale rapporto concessorio non è sufficiente l’esistenza di un atto autoritativo di investitura soggettiva del pubblico servizio, ma è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette a una disciplina di tipo pubblicistico.

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l’accento sul carattere della strumentalità ed accessorialità delle attività rispetto a quella pubblica in senso stretto.

Essa ha quindi indicato una serie di “indici rivelatori” del carattere pubblicistico dell’ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

- la sottoposizione ad un’attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici
- la presenza di una convenzione e/o concessione con la pubblica amministrazione
- l’apporto finanziario da parte dello Stato
- l’immanenza dell’interesse pubblico in seno all’attività economica.

Sulla base di quanto sopra riportato, si potrebbe ritenere che l’elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di “incaricato di un pubblico servizio” è rappresentato, non dalla natura giuridica assunta o detenuta dall’ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

È importante dunque tenere a mente che, ad esempio, allorché una banca svolga l’attività di concessionaria per la riscossione delle imposte, in quella veste essa è incaricata di pubblico servizio. Bisogna perciò sempre esaminare con attenzione il tipo di rapporto che si instaura con un ente terzo e nel caso di dubbio sulla natura giuridica, rivolgersi immediatamente alla funzione specifica per approfondimenti e chiarimenti.

### **3.3. Le fattispecie di reato richiamate dal D.Lgs 231/01**

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 della società, è funzionale alla prevenzione dei reati stessi e quindi all’intero sistema di controllo previsto dal decreto.

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del d.lgs. n. 231/2001, si riporta, qui di seguito, una breve descrizione dei reati richiamati dagli art. 24 (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) e art.25 (concussione e corruzione) del D.Lgs. 231/01.

### **3.3.1. Malversazione a danno dello Stato o dell'Unione Europea (Art. 316 bis c.p.)**

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). La pena prevista per il reato in oggetto è la reclusione da sei mesi a quattro anni.

Per i dipendenti il reato in oggetto potrà configurarsi nell'ipotesi in cui le sovvenzioni siano erogate a favore della Azienda perché ne fruisca direttamente ovvero perché si faccia tramite della loro distribuzione ai privati destinatari dell'erogazione.

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

#### **Esempio**

*I dipendenti dell'azienda, cui sia stata affidata la gestione di un finanziamento pubblico, utilizzano i fondi per scopi diversi da quelli per i quali il finanziamento è stato erogato (ad esempio, fondi ricevuti per scopi di formazione del personale dipendente vengono utilizzati per coprire le spese di corsi già effettuati autonomamente dalla società).*

### **3.3.2. Indebita percezione di erogazioni a danno dello Stato (Art. 316 ter c.p.)**

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

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Il reato in oggetto è punito con la reclusione da sei mesi a tre anni. Tuttavia, quando la somma indebitamente percepita è pari o inferiore a 3.999,96 Euro, si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5.164 Euro a 25.822 Euro. Tale sanzione non può, comunque, superare il triplo del beneficio conseguito.

Il reato di cui all'art. 316-ter c.p. potrebbe configurarsi in capo alla società sotto forma di concorso nel reato. In particolare, eventuali comportamenti scorretti dell'azienda nel rilascio di garanzie fidejussorie necessarie per l'ottenimento di erogazioni pubbliche da parte di propri clienti garantiti possono integrare gli estremi di un concorso nel reato previsto dal Decreto.

#### **Esempio**

*Un funzionario aziendale rilascia, in violazione della procedura aziendale adottata, una garanzia fidejussoria necessaria per l'ottenimento di un finanziamento pubblico da parte di un proprio Cliente, pur essendo a conoscenza che il garantito non possiede i requisiti di legge per l'ottenimento dell'erogazione pubblica.*

### **3.3.3. Truffa in danno dello Stato o di altro Ente Pubblico o dell'Unione Europea (Art. 640 – Comma 2, numero 1, c.p.)**

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro ente pubblico o all'Unione Europea). La pena prevista è quella della reclusione da uno a cinque anni e della multa da 309 Euro a 1.549 Euro.

#### **Esempio**

*Nella predisposizione di documenti o dati per la partecipazione a procedure di gara, la società fornisce alla Pubblica Amministrazione informazioni non veritiere.*

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

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

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

La pena prevista per il reato in oggetto e quella della reclusione da uno a sei anni.

**Esempio**

*A titolo esemplificativo, si veda il caso precedente di cui all'art. 640 c.p.: la finalità deve consistere nell'ottenimento di un finanziamento o contributo pubblico.*

**3.3.5. Frode informatica in danno dello Stato o di altro Ente Pubblico (Art. 640 ter c.p.)**

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

Tale reato è punito con la reclusione da sei mesi a tre anni e con la multa da 51 Euro a 1.032 Euro ovvero, 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 o, infine, se il fatto è commesso con abuso della qualità di operatore del sistema, con la reclusione da uno a cinque anni e con la multa da 309 Euro a 1.549 Euro.

**Esempio**

*In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, l'azienda violasse il sistema informatico della Pubblica Amministrazione al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.*

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

Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere o altro funzionario).

Il reato in oggetto è punito con la pena della reclusione da un minimo di tre anni ad un massimo di venti per il caso più grave (ossia, se dal fatto deriva l'ingiusta condanna di taluno alla reclusione superiore a cinque anni o all'ergastolo).

**Esempio**

*Un dirigente versa denaro ad un cancelliere del Tribunale affinché accetti, seppur fuori termine, delle memorie o delle produzioni documentali, consentendo quindi di superare i limiti temporali previsti dal codice di procedura penale a tutto vantaggio della propria difesa.*

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

Tale ipotesi di reato rappresenta una "forma anticipata" del reato di corruzione. In particolare il reato di istigazione alla corruzione si configura tutte le volte in cui, in presenza di un comportamento finalizzato alla commissione di un reato di corruzione, questa non si perfezioni in quanto il pubblico ufficiale rifiuta l'offerta o la promessa non dovuta e illecitamente avanzatagli per indurlo a compiere ovvero ad omettere o ritardare un atto del suo ufficio.

Tale reato è punito con le pene previste per i reati di cui agli artt. 318 e 319 c.p., ridotte di un terzo (ossia, da un minimo di 2 mesi ad un massimo di un anno e mezzo circa di reclusione).

**Esempio**

*Si veda il caso enunciato relativamente al reato di corruzione per un atto d'ufficio o contrario ai doveri d'ufficio con conseguente rifiuto dell'offerta del dipendente da parte del pubblico ufficiale.*

**3.4. Le attività sensibili relative ai reati contro la Pubblica Amministrazione**

Sulla base della normativa attualmente in vigore e dalle analisi svolte, le Aree Sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere comportamenti illeciti nei rapporti con la Pubblica Amministrazione riguardano in via generale le seguenti Attività Sensibili.

**Attività Sensibili**

- Nelle quali si instauri un rapporto contrattuale con la P.A.

*A titolo d'esempio si considerino i processi di aggiudicazione e gestione di commesse pubbliche, i contratti di finanziamento su progetti di rilievo pubblicistico, i rapporti con uffici del Ministero del Lavoro o Enti previdenziali.*

- Nelle quali si instauri un rapporto con le istituzioni e le Autorità di Vigilanza

- Relative alla gestione degli acquisti, delle consulenze e delle liberalità

- Che comportino la gestione delle verifiche e delle ispezioni

- Che comportino la gestione dell'erogazione del credito anche attraverso fondi pubblici, sia nella fase d'acquisizione che dell'erogazione di contributi, in qualsiasi modo denominati, destinati a pubbliche finalità, sia nello svolgimento di funzioni in regime di concessione, in quanto regolate da norme di diritto pubblico ed atti autoritativi.

*A titolo d'esempio, si considerino i processi di acquisizione e gestione di finanziamenti agevolati per interventi formativi, finanziamenti a Clientela con agevolazioni pubbliche, rapporti di Tesoreria con Enti della P.A., riscossione tributi, servizi di concessione, pagamento e custodia per conto della P.A. (pensioni, etc).*

- Che comportino la gestione dei servizi informatici.

### 3.5. Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni nello svolgimento delle proprie attività commerciali, finanziarie, di informazione e di controllo sia in favore della società stessa sia in favore della Clientela.

- **Servizio Acquisti - Ufficio Acquisti**

*L'attività presenta profili di rischio nella gestione degli acquisti dell'Azienda e per l'approvvigionamento dei beni e servizi a favore di essa*

- **Consiglio di Amministrazione**

*I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili, nonché le attività relative alla gestione dei valori svolte sia per conto della Azienda sia per conto della Clientela*

- **Servizio Audit**

*Considerata la funzione non operativa dell'Internal Audit, questa, tuttavia, potrebbe presentare il rischio di colpa in vigilando, consistente nel mancato o non corretto controllo delle attività svolte all'interno della Azienda e che coinvolgano le Autorità amministrative*

- **Servizio Amministrazione e Controllo**

*L'attività di questa funzione si considera a rischio per la gestione della corretta rappresentazione dei risultati economici della Azienda, gli adempimenti fiscali ed i rapporti con le Autorità di Vigilanza*

Ai fini della commissione dei reati contro la Pubblica Amministrazione è necessaria l'instaurazione di rapporti di natura contrattuale e non contrattuale con Pubblici Ufficiali e/o Incaricati di Pubblico Servizio appartenenti alla Pubblica Amministrazione, agli enti pubblici e/o ai soggetti ad essi assimilati facenti parte dello Stato italiano, delle Comunità Europee e degli Stati esteri.

Nel corso dell'attività di analisi condotta nell'ambito delle varie funzioni aziendali, sono state individuate le "Aree a Rischio Reato" suddivise in:

<b>AREE A RISCHIO "REATO DIRETTO"</b>	Ossia nel cui ambito sono poste in essere attività che per effetto di contatti diretti con i funzionari pubblici e/o incaricati di un pubblico servizio, comportino il rischio di commissione di uno o più dei reati contro la P.A.
<b>AREE A RISCHIO "STRUMENTALI"</b>	Alla realizzazione dei reati contro la P.A., ossia aree che gestiscono strumenti di tipo finanziario e/o mezzi sostitutivi che possono supportare la commissione dei reati nelle aree a rischio reato diretto.

In considerazione delle attività aziendali e delle tipologie di contatti con la Pubblica Amministrazione, sono state individuate le seguenti aree a rischio. Si precisa che laddove un'area presenta le caratteristiche sia di area a rischio diretto che strumentale, onde evitare duplicazioni, la stessa è stata classificata sotto la prima tipologia.

Nell'ambito di ciascuna "area a rischio reato diretto" sono stati individuate le principali "attività sensibili", ossia quelle attività, all'interno di tali aree, al cui svolgimento è connesso il rischio di commissione dei reati considerando la sussistenza di rapporti diretti con i soggetti sopra definiti come Pubblica Amministrazione.

Di seguito si riportano le "aree a rischio reato diretto" con una breve descrizione delle attività che le compongono e l'elenco delle "aree a rischio strumentale". Si tratta di un elenco di sintesi, in continuo divenire proprio per le caratteristiche insite nel Modello 231 stesso, di tipo dinamico.

Relazioni esterne ed istituzionali	<ul style="list-style-type: none"> <li>– Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, dei controlli e/o degli accertamenti</li> <li>– Gestione adempimenti amministrativi e fiscali, rapporti con Uffici Tributarî (dichiarazione dei redditi, dichiarazione Iva, dichiarazione sostituto d'imposta)</li> </ul>
Area fiscale	–
Affari legali	<ul style="list-style-type: none"> <li>– Avvio di procedimenti giudiziari o stragiudiziali dinanzi alle competenti autorità</li> <li>– Gestione dei rapporti con gli enti pubblici competenti relativamente a autorizzazioni sanitarie, denunce per tributi locali, violazioni del Codice della Strada, rifiuti e pratiche varie</li> <li>– Gestione dell'attività di contenzioso in tutti i gradi di giudizio anche attraverso l'ausilio di legali esteri</li> </ul>
Gestione erogazioni pubbliche	<ul style="list-style-type: none"> <li>– Gestione delle domande avente ad oggetto la richiesta di finanziamenti, contributi ed aiuti pubblici nonché collazione e predisposizione della documentazione a supporto della domanda</li> <li>– Gestione dell'utilizzo dei finanziamenti, contributi ed aiuti pubblici conseguiti dalle competenti</li> </ul>

	<ul style="list-style-type: none"> <li>– autorità nazionali e comunitarie</li> <li>– Gestione dell'attività di rendicontazione delle attività svolte all'ente pubblico erogatore</li> <li>– Gestione delle eventuali verifiche ispettive da parte delle competenti autorità nazionali e comunitarie al fine di verificare la destinazione dei contributi e dei finanziamenti ottenuti</li> </ul>
Gestione dei trattamenti previdenziali del personale	<ul style="list-style-type: none"> <li>– Si tratta dell'attività di gestione e amministrazione degli aspetti retributivi e previdenziali connessi al personale dirigente, dipendente e ai collaboratori esterni e dei relativi rapporti con enti previdenziali ed assistenziali</li> </ul>
Gestione della salute e sicurezza	<ul style="list-style-type: none"> <li>– Predisposizione e trasmissione alle competenti autorità della documentazione necessaria al fine di porre in essere i relativi adempimenti inerenti la salute e sicurezza sul lavoro (D.Lgs. 81/08 e successive modifiche)</li> <li>– Gestione dei rapporti con gli enti sanitari competenti in relazione alle tematiche inerenti la salute e sicurezza sul lavoro</li> <li>– Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, controlli e/o accertamenti</li> </ul>
Amministrazione	<ul style="list-style-type: none"> <li>– Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, controlli e/o accertamenti</li> </ul>

AREA A RISCHIO C.D. "STRUMENTALI"	SISTEMI INFORMATIVI
	FINANZA E TESORERIA
	CONTABILITA' FORNITORI
	CONTABILITA' CLIENTI
	GESTIONE OMAGGI E REGALIE
	ACQUISTI MATERIALI TECNICI E VARI

Eventuali integrazioni delle suddette aree a rischio reato potranno essere proposte alla Direzione Aziendale dall'Organismo di Vigilanza e dagli altri organi di controllo della Azienda per effetto dell'evoluzione dell'attività di impresa e conseguentemente di eventuali modifiche dell'attività svolta dalle singole funzioni aziendali.

### 3.6. Principi e regole di comportamento

Si individuano qui di seguito i principi che informano le specifiche procedure interne della Azienda previste in relazione a qualsiasi operazione/attività che coinvolga un ente della Pubblica Amministrazione, nonché le regole di condotta che sottendono alle specifiche previsioni di comportamento elaborate dalla Azienda in relazione a tale ambito di applicazione.

Si stabilisce pertanto che tutte le regole, i processi e le prassi operative nei rapporti con la P.A. devono rispettare i principi e le regole di comportamento nel seguito delineate.

#### Principi

Tutte le operazioni/attività che coinvolgono in qualsiasi modo un ente della Pubblica Amministrazione devono essere poste in essere nel pieno rispetto delle leggi vigenti, del Codice Etico e del Codice di Comportamento Interno, delle regole contenute nel presente Modello, delle policy e delle procedure aziendali, dei valori e delle politiche della Azienda.

La struttura aziendale è articolata in modo tale da soddisfare i requisiti fondamentali di formalizzazione, chiarezza, comunicazione e separazione dei ruoli richiesti in generale nel Decreto e di peculiare importanza nella gestione dei rapporti con la Pubblica Amministrazione, in particolare per ciò che concerne l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

La Azienda si dota di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, mansionari etc.) improntati a principi generali di:

- Conoscibilità all'interno della Azienda (ed eventualmente anche nei confronti di eventuali altre società del Gruppo)

- Chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri
- Chiara descrizione delle linee di riporto.

A tal fine, le procedure interne aziendali sono strutturate in modo da garantire in generale per ciascun processo ed in particolare nei rapporti con la Pubblica Amministrazione:

- Una distinzione, quanto più possibile netta, tra il soggetto che lo avvia a livello decisionale, il soggetto che lo esegue e lo porta a termine ed il soggetto che lo controlla
- La tracciabilità scritta di ciascuna fase rilevante
- Un adeguato livello di formalizzazione
- Che i sistemi premianti e/o di incentivazione dei soggetti che hanno poteri di spesa e facoltà decisionali non siano commisurati al raggiungimento di risultati sostanzialmente irraggiungibili.

### **Il sistema di deleghe e procure**

In linea di principio il sistema di deleghe e procure, formalizzato in apposito documento approvato dal Consiglio di Amministrazione, stabilisce espressamente le facoltà di autonomia gestionale per natura di spesa e di impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione.

Si intende per “delega” quell’atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per “procura” il negozio giuridico unilaterale con cui una società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei reati sono i seguenti:

- Le funzioni che intrattengono per conto della Azienda rapporti con la P.A. devono essere individuate e preferibilmente dotate di delega formale in tal senso
- Le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell’organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi
- Ciascuna delega deve definire in modo specifico:
  - I poteri del delegato
  - Il soggetto (organo o individuo) cui il delegato riporta gerarchicamente
- I poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali
- Il delegato deve disporre di eventuali poteri di spesa adeguati alle funzioni conferitegli
- Presenza di una procedura interna che permetta l'immediata modifica, estinzione o conferimento di deleghe e procure al mutare delle mansioni, ruoli o poteri di un dipendente o membro di un organo sociale aziendale

L’Organismo di Vigilanza verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni alla Azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

### **Regole di comportamento**

Le seguenti regole di carattere generale si applicano sia ai Dipendenti e agli Organi Sociali della società – in via diretta – sia ai Collaboratori esterni e ai Partner, anche in forza di apposite clausole contrattuali.

E’ fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001); sono altresì proibite le violazioni ai principi procedurali ed alle procedure aziendali previsti nella presente Parte Speciale.

E’ obbligatorio segnalare all’Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

In tutte le operazioni/attività della Azienda che coinvolgano un ente della Pubblica Amministrazione, è fatto espresso divieto ai Destinatari di:

- Effettuare elargizioni in danaro a pubblici funzionari.
- Distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale e, in particolare, è vietata qualsiasi forma di regalo o di gratuita prestazione in favore di pubblici funzionari o di soggetti ad essi legati da un vincolo familiare che possa anche solo apparire come atto ad influenzare l’indipendenza di giudizio di tali soggetti ovvero

tesa ad assicurare un qualsiasi vantaggio improprio per l'azienda. Gli omaggi consentiti non superano il valore di Euro 150 e sono volti a promuovere iniziative di carattere benefico/culturale. Le liberalità che non rispecchino questo valore devono essere interpretate come sponsorizzazioni ed in quanto tali devono essere autorizzate e trattate secondo le procedure aziendali allo scopo previste.

- Accordare vantaggi di qualsiasi natura in favore di rappresentanti di enti della Pubblica Amministrazione che possano determinare le stesse conseguenze di cui al punto precedente.
- Ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque sia o intenda entrare in rapporto con la Società e voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite dall'azienda o, comunque, un trattamento più favorevole di quello dovuto.
- Eseguire prestazioni o riconoscere compensi in favore dei collaboratori esterni e dei partner che non siano adeguatamente giustificati in ragione del rapporto contrattuale in essere con l'azienda.
- Presentare dichiarazioni non veritiere a enti pubblici nazionali e/o comunitari al fine di conseguire o far conseguire erogazioni, contributi o finanziamenti agevolati.
- Destinare eventuali somme ricevute da enti pubblici nazionali e/o comunitari per scopi diversi da quelli a cui originariamente erano destinati.
- Accedere alla rete informatica aziendale in assenza dell'utilizzo di doppia chiave asimmetrica; composta da user ID e da password personale, che consenta all'operatore di accedere alla rete limitatamente alla fase della procedura di sua competenza; ciò sia che l'accesso sia finalizzato per l'inserimento/modifica o per la comunicazione a/da terzi di dati in essa contenuti, sia per qualunque intervento sui programmi destinati ad elaborarli, riferiti alla Clientela in generale e agli enti della Pubblica Amministrazione in particolare.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nella parte generale del Modello 231 e nella presente parte speciale.

In generale, il sistema di organizzazione, gestione e controllo della Azienda deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte ed, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali, devono conoscere e rispettare:

- La normativa italiana applicabile alle attività svolte
- Il Codice Etico Aziendale
- Il presente Modello Organizzativo
- Le procedure e le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della Azienda.

A tale proposito la Azienda deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, etc.) improntati a principi generali di:

- Conoscibilità all'interno della Azienda
- Delimitazione dei ruoli, con una descrizione dei compiti di ciascuna funzione e dei relativi poteri.

In genere, le procedure interne sono caratterizzate dai seguenti elementi:

- Individuazione all'interno di ciascun processo, del soggetto che lo promuove (impulso decisionale), del soggetto che lo esegue e lo conclude, e del soggetto che lo controlla.
- Adeguato livello di formalizzazione e documentazione delle diverse fasi della procedura.

### **3.7. Principi e norme generali di comportamento**

I soggetti destinatari della presente Parte Speciale coinvolti nelle attività elencate nei paragrafi precedenti devono rispettare principi e norme di comportamento di seguito dettate, nel rispetto degli obblighi normativi, delle procedure aziendali e del Codice Etico aziendale.

Coerentemente con i principi del Codice Etico, i rapporti tra la Azienda e la Pubblica Amministrazione devono essere condotti in conformità alla legge e nel rispetto dei principi di lealtà, correttezza, trasparenza e verificabilità.

Si sottolinea che è assolutamente vietato:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, assunti individualmente o nel particolare contesto in cui si collocano, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001).

- Promettere, offrire o acconsentire all'elargizione di denaro o altre utilità (beni materiali, servizi, etc.) a pubblici ufficiali o incaricati di pubblico servizio, o a loro familiari, che possano influenzare l'indipendenza del giudizio o indurre ad assicurare un vantaggio per la società.
- Accordare vantaggi di qualsiasi natura (promessa di assunzione, etc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al punto precedente.
- Distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale) ed in particolare, è vietata qualsiasi forma di regalo a funzionari pubblici o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o la brand image della Azienda. I regali offerti - salvo quelli di modico valore, devono essere documentati in modo adeguato per consentire le verifiche da parte dell'OdV.
- Mettere in atto o favorire operazioni in conflitto di interesse della Azienda, nonché attività in grado di interferire con la capacità di assumere decisioni imparziali nell'interesse della Azienda nel rispetto del Codice Etico e delle normative applicabili.
- Effettuare prestazioni in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi.
- Riconoscere compensi in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale.
- Effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati, o comunque utilità a carico di bilanci pubblici, e/o per partecipare a gare o simili o risultarne vincitori.
- Effettuare comunque dichiarazioni o attestazioni non veritiere ad organismi pubblici tali da indurre in errore tali soggetti, da creare un indebito profitto o vantaggio a favore della società e/o arrecare un danno all'ente pubblico.
- Destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.
- Violare i principi e le procedure aziendali previste nella presente sezione della Parte Speciale.

Al fine di scongiurare la commissione dei reati di cui alla presente sezione devono essere realizzati i seguenti presidi di controllo:

- Distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi nelle attività di predisposizione, presentazione e ricezione di dati, informazioni e documenti verso/da rappresentanti della Pubblica Amministrazione, allo scopo di evitare sovrapposizioni funzionali o eccessive concentrazioni di potere.
- Formale identificazione del soggetto deputato ad intrattenere rapporti con la PA. in relazione a ciascuna Potenziale Attività a Rischio.
- Gestione in modo trasparente e univoco di qualsiasi rapporto professionale instaurato con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio.
- Attività di reporting all' OdV di eventuali situazioni di irregolarità.

### **3.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili**

Gli Organi Sociali, gli amministratori, i dipendenti e i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali, nell'ambito delle attività da essi svolte, devono rispettare le regole ed i divieti elencati al precedente paragrafo e ai fini dell'attuazione degli stessi devono rispettare le procedure specifiche qui di seguito descritte, oltre alle Regole e Principi Generali già contenuti nella Parte Generale del Modello 231.

In particolar modo nella gestione dei rapporti con la Pubblica Amministrazione devono essere osservate, tra le altre, le regole di comportamento di seguito indicate:

- Agli Organi Sociali, Dipendenti, Consulenti e Partner che materialmente intrattengono rapporti con la PA per conto della Azienda deve essere formalmente conferito potere in tal senso dalla società (con apposita delega per i membri degli organi sociali e per i dipendenti - anche tramite il responsabile, individuato in base al sistema delle comunicazioni organizzative, ovvero nel relativo contratto di servizio o di consulenza o di partnership per gli altri soggetti destinatari del Modello 231). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri elencati nella Parte Generale.

- Il responsabile individuato a rilasciare le procure deve predisporre una lista riepilogativa di tutti i Responsabili/addetti ad intrattenere rapporti con la Pubblica Amministrazione e renderla eventualmente disponibile sull'Intranet aziendale (o altro sistema di comunicazione interna).
- I contratti tra la Azienda, i Consulenti e Partner che abbiano, anche solo potenzialmente, impatto sulle Potenziali Aree a Rischio devono essere definiti per scritto in tutte le loro condizioni e termini e devono contenere clausole standard al fine di garantire il rispetto del D.Lgs. 231/2001.
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi, finanziamenti, ed in genere di benefici a carico di bilanci pubblici, devono contenere solo elementi veritieri e, l'impegno della Azienda, in caso di ottenimento degli stessi, all'effettiva utilizzazione dei fondi ottenuti secondo le finalità previste dalla specifica normativa di riferimento. In ogni caso, ciascuna delle dichiarazioni di cui al presente capo, ivi incluse le autocertificazioni ammesse dalla legge o dai bandi, devono essere corredate da documentazione idonea ad attestarne la veridicità, anche se eventualmente non richiesta dal destinatario di tali dichiarazioni.
- Alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D.Lgs. 81/08 e successive modifiche, a verifiche tributarie, INPS, etc.) devono partecipare i soggetti a ciò espressamente delegati, dando avviso dell'avvio dell'ispezione/accertamento al Legale rappresentante ed all'OdV. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati appositi verbali. Nel caso il verbale conclusivo evidenziasse criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile coinvolto.
- La stipulazione di contratti/convenzioni con soggetti pubblici da parte della Azienda a seguito della partecipazione a procedure ad evidenza pubblica (asta pubblica, appalto-concorso, licitazione privata e trattative private) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello.
- Qualunque tipo di erogazione di fondi:
  - Deve essere deliberata previa adeguata istruttoria cui partecipino soggetti e funzioni diverse all'interno della Azienda, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni aziendali.
  - Presuppone una approfondita conoscenza della Clientela, così da consentire una valutazione della coerenza e della compatibilità dell'operazione con il profilo del Cliente, soprattutto laddove quest'ultimo non svolga attività di rilievo economico.
- Ai Collaboratori esterni e Partner che materialmente intrattengono rapporti con la P.A. per conto della Azienda, deve essere formalmente conferito potere in tal senso dalla Azienda stessa, con apposita clausola contrattuale.
- L'Organismo di Vigilanza deve essere informato con nota scritta di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A.
- I contratti tra la Società e i Collaboratori esterni e i Partner devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti.
- I Collaboratori esterni devono essere scelti con metodi trasparenti e secondo specifica procedura aziendale, nel rispetto della quale la selezione deve avvenire tra i Collaboratori esterni accreditati; le richieste di spesa eventualmente rivolte a soggetti non accreditati dovranno essere accompagnate da adeguata motivazione.
- I Partner devono essere scelti con metodi trasparenti e secondo specifica procedura (ad esempio: utilizzando apposite check list o una procedura formalizzata).
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di concessioni, autorizzazioni o licenze devono contenere solo elementi assolutamente veritieri.
- Alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D.Lgs. 81/08, verifiche tributarie, INPS, Autorità di vigilanza ecc.) devono partecipare i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali che verranno conservati dall'Organismo di Vigilanza.

### **3.9. I controlli dell'Organismo di Vigilanza**

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui agli artt. 24 e 25 del Decreto, commessi nell'interesse o a vantaggio della Azienda, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui agli artt. 24 e 25 del Decreto sono i seguenti:

- Proporre che vengano costantemente aggiornate le procedure aziendali per prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione, di cui alla presente Parte Speciale; con riferimento a tale punto l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di commissione dei suddetti reati, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere; o proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale.
- Monitorare sul rispetto delle procedure interne per la prevenzione dei reati oggetto della presente Parte Speciale. Sulla base dei flussi informativi ricevuti l'Organismo di Vigilanza condurrà verifiche mirate su determinate operazioni effettuate nell'ambito delle Aree Sensibili, volte ad accertare da un lato il rispetto di quanto stabilito nel Modello e nei protocolli, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili.
- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute. L'Organismo di Vigilanza, inoltre, è tenuto alla conservazione dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

#### **4. – SEZIONE “B” – REATI SOCIETARI**

##### **4.1. Introduzione e funzione della parte speciale dedicata ai reati societari**

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Societari della Azienda, nonché dai suoi Collaboratori esterni e dai suoi Partner, come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i Destinatari, conducano comportamenti conformi a quanto ivi descritto al fine di impedire il verificarsi degli illeciti di cui all'art. 25-ter del Decreto.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all’Organismo di Vigilanza - e ai responsabili delle funzioni aziendali che cooperano con tale organismo - gli strumenti esecutivi per esercitare le attività di controllo, di monitoraggio e di verifica.

La Azienda adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione delle fattispecie delittuose di seguito descritte.

##### **4.2. Le fattispecie di reato richiamate dal D.Lgs 231/01**

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 della Azienda, è funzionale alla prevenzione dei reati stessi e quindi all’intero sistema di controllo previsto dal decreto.

L’art. 25-ter del Decreto contempla la maggior parte dei reati societari che costituiscono, al momento, insieme agli abusi di mercato, i soli reati autenticamente economici di cui può essere chiamata a rispondere la Azienda e che, in quanto non occasionati dall’esercizio della specifica attività aziendale, sono qualificabili come reati generali.

Di seguito si riporta una breve descrizione dei reati societari richiamati dall’art. 25-ter ( Reati societari ) del D.Lgs. 231/01 che si ritiene potrebbero trovare manifestazione nell’ambito delle attività svolte dall’azienda.

La presente Parte Speciale si riferisce ai reati societari.

##### **4.2.1. False comunicazioni sociali (Artt. 2621 e 2622 c.c.)**

Questo reato si realizza tramite:

- l’esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l’intenzione di ingannare i soci o il pubblico;
- l’omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false od omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della Azienda o del gruppo al quale essa appartiene;
- la responsabilità si ravvisa anche nell’ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla Azienda per conto di terzi;
- il reato di cui all’articolo 2622 del codice civile è punibile a querela, salvo che si tratti di società quotate.

Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

##### **Esempio**

*Il Consiglio di Amministrazione ignora l’indicazione del responsabile amministrativo circa l’esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti a fronte della situazione di crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l’assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 del codice civile).*

##### **4.2.2. Falso in prospetto (art. 173-bis D.Lgs. n. 58 del 1998 aggiornato con D.lgs. n. 164 del 17.09.2007)**

Tale condotta criminosa consiste nell’espone, nei prospetti richiesti ai fini della sollecitazione all’investimento o dell’ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, false informazioni idonee ad indurre in errore od occultare dati o notizie.

Si precisa che:

- deve sussistere l'intenzione di ingannare i destinatari del prospetto;
- la condotta deve essere idonea a trarre in inganno i destinatari del prospetto;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.

Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

**Esempio**

*Il Consiglio di Amministrazione omette di rappresentare nel documento informativo richiesto ex lege, destinato alla pubblicazione a seguito di una sollecitazione all'investimento deliberata dagli Organi Sociali, elementi idonei a formare un giudizio veritiero sui titoli (es. elevato grado di rischio dell'investimento).*

**4.2.3. Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.)**

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, concernenti la situazione economica, patrimoniale o finanziaria della società, al fine di conseguire per sé o per altri un ingiusto profitto.

La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.

Soggetti attivi sono i responsabili della società di revisione (reato proprio). Pertanto tale reato non è configurabile in capo alla Azienda.

Tuttavia, i componenti degli organi di amministrazione e di controllo dell'Azienda e i suoi dipendenti possono essere coinvolti a titolo di concorso nel reato. Infatti, ai sensi dell'art. 110 c.p. è ipotizzabile il concorso eventuale degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del responsabile della società di revisione.

**Esempio**

*Un funzionario aziendale collabora con la società di revisione in sede di valutazione di cespiti patrimoniali aziendali in modo da occultarne le gravi perdite, così rappresentando una situazione economica, patrimoniale e finanziaria della società tale da sottrarla da eventuali giudizi pregiudizievoli.*

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

Il reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione.

Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

**Esempio**

*Un funzionario della Azienda rifiuta di fornire alla società di revisione i documenti richiesti per l'espletamento dell'incarico, quali, ad esempio, quelli concernenti le azioni legali intraprese dalla società per il recupero di crediti.*

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

Tale ipotesi si ha quando viene formato o aumentato fittiziamente il capitale della Azienda mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; vengono sottoscritte reciprocamente azioni o quote; vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della Azienda nel caso di trasformazione.

Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

**Esempio**

*L'Assemblea della Azienda, su proposta del Consiglio di Amministrazione, delibera l'aumento del capitale sociale con un conferimento di beni sopravvalutati in modo rilevante.*

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

La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

**Esempio**

*L'Assemblea della Azienda, su proposta del Consiglio di Amministrazione, delibera la compensazione di un debito di un socio nei confronti della società con il credito da conferimento che quest'ultima vanta nei confronti del socio medesimo, attuando di fatto una restituzione indebita del conferimento.*

#### **4.2.7. Illegale ripartizioni degli utili o delle riserve (art. 2627 c.c.)**

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva; ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite. Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato, Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

##### **Esempio**

*L'Assemblea della Azienda, su proposta del Consiglio di Amministrazione, delibera la distribuzione di dividendi che costituiscono, non un utile di esercizio, ma fondi non distribuibili perché destinati dalla legge a riserva legale.*

#### **4.2.8. Illecite operazioni sulle azioni o quote sociali o delle società controllate (art. 2628 c.c.)**

Questo reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Si fa presente che 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. Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

##### **Esempio**

*L'Organo amministrativo procede all'acquisto o alla sottoscrizione di azioni della società o di una società controllante fuori dai casi di cui all'artt. 2357, 2359-bis del codice civile, cagionando in tal modo una lesione del patrimonio sociale.*

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

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

##### **Esempio**

*L'organo amministrativo delibera una riduzione del capitale sociale senza osservare i presupposti richiesti dalla legge, cagionando in tal modo un danno ai creditori sociali.*

#### **4.2.10. Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)**

Il reato si perfeziona nel caso in cui l'amministratore di una società con azioni quotate non comunichi agli altri amministratori e al collegio sindacale un interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, cagionando a seguito di tale omissione un danno alla società o a terzi. Tale ipotesi di reato non può configurarsi in capo all'azienda se questa non è quotata.

##### **Esempio**

*Un amministratore di una società quotata, nel corso di una riunione del Consiglio di Amministrazione della stessa, convocato per valutare e deliberare un'acquisizione societaria ad un prezzo eccessivo rispetto al reale valore della target, non comunica agli altri consiglieri che sua moglie è proprietaria di una partecipazione di maggioranza nella società oggetto dell'acquisizione.*

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

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda ma riguardando un'ipotesi di liquidazione volontaria o coatta.

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

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Tale ipotesi di reato potrebbe configurarsi in capo alla Azienda.

##### **Esempio**

*Il Consiglio di Amministrazione della Azienda, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinante anche del socio di maggioranza, predispose e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso Consiglio di Amministrazione intende acquisire, in modo da ricavarne un indiretto profitto.*

#### **4.2.13. Corruzione tra privati (art. 2635 c.c.)**

Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate 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 delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

Tale ipotesi di reato potrebbe configurarsi in capo alla società.

#### **4.3. Le attività sensibili relative ai reati societari**

L'art. 6, comma 2, lett. a) del D.Lgs. 231/01 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Azienda nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Nell'ambito di ciascun reato, sulla base della mappatura di dettaglio delle aree aziendali a rischio, sono state individuate le attività da ritenersi maggiormente "sensibili" come di seguito riportato.

##### **False comunicazioni sociali (art. 2621 c.c.)**

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

Gli altri reati previsti dall'art. 25-ter non sono stati, allo stato attuale, valutati rilevanti in quanto la probabilità di commissione di tali reati è ritenuta remota.

La Azienda si riserva di aggiornare il presente Modello 231 nel caso in cui dovesse emergere la significatività di uno o più degli altri reati sopra elencati.

Principali Aree a rischio e attività sensibili interessate:

Gestione della Contabilità Generale:

- **Imputazione delle scritture contabili** in contabilità generale
- **Verifiche sui dati contabili** immessi a sistema e quelli inviati al consulente esterno
- **Predisposizione di bilanci e documentazione di natura contabile:** si tratta delle attività relative alle chiusure contabili, alla contabilizzazione dei dati e alla predisposizione del bilancio d'esercizio della Azienda e dei relativi allegati
- **Predisposizione di documenti** ai fini delle delibere assembleari e delle decisioni della Direzione aziendale: si tratta delle attività di predisposizione della documentazione relativa all'oggetto dell'Assemblea e della Direzione

aziendale per consentire a questi ultimi di esprimersi sulle materie di propria competenza sottoposte ad approvazione

- **Gestione delle comunicazioni verso soci:** si tratta dell'attività di predisposizione della documentazione oggetto di comunicazioni verso soci.

Nel caso in cui esponenti della Azienda si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

- a) degli standard di controllo generali,
- b) dei principi di comportamento individuati nel Codice Etico,
- c) di quanto regolamentato dalla documentazione e dagli atti aziendali,
- d) delle disposizioni di legge.

E' responsabilità del legale rappresentante segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni da apportare alla Parte Speciale, in accordo a quanto previsto dalla Parte Generale.

#### **4.4. Organi e funzioni aziendali coinvolte**

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni aziendali nello svolgimento delle proprie attività commerciali, finanziarie, di informazione e di controllo sia in favore della società stessa sia in favore della Clientela.

##### **Consiglio di Amministrazione**

I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili, nonché le attività relative alla gestione dei valori svolte sia per conto della Azienda sia per conto della clientela.

##### **Servizio Audit**

Considerata la funzione non operativa dell'Internal Audit, questa, tuttavia, potrebbe presentare il rischio di colpa in vigilando, consistente nel mancato o non corretto controllo delle attività svolte all'interno dell'azienda e che coinvolgono le Autorità amministrative.

##### **Servizio Amministrazione e Controllo**

L'attività di questa funzione si considera a rischio per la gestione della corretta rappresentazione dei risultati economici, degli adempimenti fiscali ed i rapporti con le Autorità di Vigilanza.

#### **4.5. Principi e regole di comportamento**

Per quanto concerne le fattispecie criminose che si riferiscono ai documenti contabili ed ai controlli delle Autorità di vigilanza, si rileva che la Azienda si pone in una posizione privilegiata dal punto di vista della prevenzione e della corretta attuazione dei precetti normativi, in quanto risulta destinataria di una disciplina speciale che impone la procedimentalizzazione dell'intera fase di elaborazione di detta documentazione, nonché una serie di obblighi ed adempimenti in relazione ai rapporti con le autorità, con la conseguenza che le modalità di gestione del rischio dei reati qui considerati risultano replicare comportamenti già consolidati nella prassi societaria o, comunque, derivanti dall'applicazione delle norme primarie e regolamentari vigenti.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole individuate dal presente Modello, i destinatari, per quanto di rispettiva competenza, sono tenuti a conoscere e a rispettare puntualmente, oltre alle norme di legge e di regolamento di volta in volta applicabili, tutta la normativa interna aziendale relativa al sistema amministrativo, finanziario e contabile.

I destinatari, inoltre, sono tenuti ad operare sulla base della best practice cui la Azienda si ispira nell'esercizio delle proprie funzioni, sul fondamento che qualsiasi condotta attiva od omissiva posta in essere in violazione diretta od indiretta dei principi normativi e delle regole procedurali interne che attengono alla formazione della documentazione contabile ed alla rappresentazione esterna, così come all'esercizio delle attività di controllo e di vigilanza è da considerare come commessa in danno della Azienda stessa.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, le politiche e le procedure aziendali nonché le regole contenute nel Modello 231 e nella presente parte speciale operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda.

In generale, il sistema di organizzazione, gestione e controllo della Azienda deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte ed, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Azienda, devono conoscere e rispettare:

- La normativa italiana e straniera applicabile alle attività svolte
- Il Codice Etico Aziendale ed eventuale Appendice Applicativa
- Il presente Modello 231
- Le procedure e le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della Azienda.

#### **4.6. Principi e norme generali di comportamento**

La presente Parte Speciale è inerente alle condotte poste in essere dai Soggetti destinatari del Modello 231 che operano, in particolare, nelle aree a Rischio Reato e nello svolgimento delle attività sensibili.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale ed al fine di perseguire la prevenzione dei Reati Societari è fatto espresso divieto a tutti i Soggetti destinatari del Modello 231 di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-ter del D.Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale.

Con riferimento a quanto espresso sopra la Azienda obbliga i suoi Amministratori, dipendenti e soggetti terzi che agiscono in rappresentanza della Azienda al rispetto, in particolare, dei seguenti principi:

- I bilanci e le comunicazioni sociali previsti dalla Legge devono essere redatti con chiarezza e rappresentare in modo corretto e veritiero la situazione patrimoniale, economica e finanziaria della società;
- È vietato, anche mediante condotte dissimulate, restituire i conferimenti effettuati dai soci o liberarli dall'obbligo di eseguirli, fuori dai casi di legittima riduzione del capitale sociale;
- È vietato ripartire utili non effettivamente conseguiti o distribuire riserve indisponibili;
- È vietato effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di Legge a tutela dei creditori;
- È vietato formare od aumentare fittiziamente il capitale delle Azienda, mediante attribuzione di quote per somma inferiore al loro valore nominale, sottoscrizione reciproca di quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio delle Azienda in caso di trasformazione.

Quanti venissero a conoscenza di omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, sono tenuti a riferire i fatti al responsabile individuato nel Legale rappresentante e all'Organismo di Vigilanza.

Per ogni operazione contabile deve essere conservata agli atti sociali un'adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

- L'agevole registrazione contabile
- L'individuazione dei diversi livelli di responsabilità
- La ricostruzione accurata dell'operazione, anche al fine di ridurre la probabilità di errori interpretativi

Le operazioni o i fatti gestionali sensibili e/o rilevanti devono essere documentati, coerenti e congrui, così che in ogni momento sia possibile identificare la responsabilità di chi ha operato (valutato, deciso, autorizzato, effettuato, rilevato nei libri, controllato l'operazione). Le responsabilità di ciascuna operazione/processo aziendale devono essere chiaramente e formalmente definite.

#### **4.7. Principi di riferimento speciali relativi alla regolamentazione delle attività sensibili**

Gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Azienda, dovranno tener conto, oltre a quanto precedentemente

descritto e relativamente ad ognuna delle fattispecie di reato ritenute rilevanti per la Società, delle previsioni di seguito indicate:

**False comunicazioni sociali (art. 2621 c.c.)**

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

Ai fini di prevenire i reati di false comunicazioni sociali e di false comunicazioni sociali in danno della Azienda, dei soci o dei creditori, i soggetti sopra indicati hanno l'espresso obbligo di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Azienda.

A tale riguardo, deve essere loro cura, a titolo esemplificativo, astenersi da:

- a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
- b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Azienda;
- c) porre la massima attenzione e accuratezza nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni utilizzati in modo tale da fornire una presentazione veritiera e corretta corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Azienda e sull'evoluzione della sua attività.

Inoltre, gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Azienda, dovranno tener conto, oltre a quanto precedentemente definito delle procedure e regole aziendali che prevedono:

- Il rispetto del Codice Etico e delle sue specifiche previsioni riguardanti il corretto comportamento di tutti i soggetti coinvolti nelle attività di formazione del bilancio o di altri documenti simili, quali ad esempio:
  - a) Massima collaborazione, veridicità, autenticità ed originalità della documentazione e delle informazioni trattate;
  - b) Chiarezza e correttezza della rappresentazione patrimoniale e finanziaria della Azienda;
  - c) Completezza, segnalazione di eventuali omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, etc..
- Il rispetto del calendario di chiusura, finalizzato alla redazione del bilancio indicante:
  - a) Data di chiusura dei periodi contabili
  - b) Data di chiusura delle scritture contabili
  - c) Data di predisposizione della Bozza del Bilancio e del Bilancio Definitivo
- La chiara definizione della responsabilità della veridicità, autenticità ed originalità della documentazione e delle informazioni e dei dati forniti dal Responsabile della determinazione delle varie poste/fondi;
- Il supporto documentale a corredo delle informazioni e dei dati forniti dal Responsabile di cui al punto precedente;
- Il controllo, da parte del consulente esterno incaricato nella predisposizione del bilancio delle voci aggregate di Bilancio confrontandole con quelle dell'anno precedente, mantenendo evidenza del riscontro effettuato e delle eventuali motivazioni relative a scostamenti anomali;
- La tracciabilità informatica delle operazioni effettuate;
- La tracciabilità dell'invio della bozza del Bilancio, alcuni giorni precedenti l'approvazione da parte del Presidente per permettere allo stesso la verifica delle connotazioni essenziali del bilancio prima che sia sottoposto all'Assemblea per l'approvazione.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Societari aziendali (e dei Dipendenti e Collaboratori esterni nella misura necessaria alla funzioni dagli stessi svolte) di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-ter del D.Lgs. n. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

La presente Parte Speciale prevede, conseguentemente, l'espreso obbligo a carico dei soggetti sopra indicati di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Azienda;
2. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3. assicurare il regolare funzionamento degli Organi Societari, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
4. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non fraponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

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

- con riferimento al precedente punto 1:
  - rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della Azienda;
  - omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Azienda;
- con riferimento al precedente punto 2:
  - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
  - ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
  - acquistare o sottoscrivere azioni della società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
  - effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
  - procedere a formazione e/o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- con riferimento al precedente punto 3:
  - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione della gestione sociale da parte del collegio sindacale o della società di revisione o che comunque la ostacolino;
  - determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- con riferimento al precedente punto 4:
  - omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di vigilanza cui è soggetta l'attività aziendale, nonché omettere di dar corso con sollecitudine all'invio dei dati e della documentazione eventualmente richiesta dalle predette autorità;
  - esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Azienda;
  - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte dell'Autorità di vigilanza.

Ai fini dell'attuazione delle regole elencate al precedente capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali specifici qui di seguito descritti:

*Predisposizione delle comunicazioni ai soci relative alla situazione economica, patrimoniale e finanziaria della Azienda*

I documenti contenenti comunicazioni ai soci relative alla situazione economica, patrimoniale e finanziaria della Azienda devono essere redatti in base alle specifiche procedure aziendali in essere che:

- determinano con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire ed i controlli che devono essere svolti su detti dati e notizie, nonché i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili;
- prevedono la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema.

In particolare, nei processi contabili e più in generale di produzione di documenti che rappresentano situazioni economiche, finanziarie e patrimoniali della Azienda le funzioni aziendali coinvolte sono tenute al rispetto dei seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione dei compiti e delle funzioni;
- documentazione delle decisioni e dei controlli;
- accurata gestione delle notizie riservate.

*Gestione dei rapporti con la società di revisione contabile in ordine all'attività di comunicazione da parte di quest'ultima a terzi relativa alla situazione economica, patrimoniale e finanziaria della Azienda*

Nei rapporti tra la Azienda e la società di revisione contabile sono adottati i seguenti presidi:

- Gli incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, vengono conferiti alla società di revisione su proposta del Collegio Sindacale;
- È vietato il conferimento a soggetti che siano parte della rete o del network cui appartiene la società di revisione di incarichi diversi dalla revisione contabile che appaiono incompatibili con quest'ultima, in quanto suscettibili di pregiudicare l'indipendenza della società di revisione incaricata;
- L'assemblea dei soci viene informata dell'eventuale conferimento di ulteriori incarichi rispetto a quello di revisione contabile alla società di revisione incaricata nonché dell'eventuale conferimento di incarichi a soggetti che siano parte della rete o del network a cui appartiene la società di revisione.

*Operazioni relative al capitale sociale*

Tutte le operazioni sul capitale sociale nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle regole di corporate governance e delle procedure aziendali e/o di gruppo predisposte.

*Predisposizione delle comunicazioni alle Autorità di vigilanza e gestione dei rapporti con le stesse*

Con riferimento alle attività societarie soggette alla vigilanza di pubbliche autorità, in base alle specifiche normative applicabili, al fine di prevenire la commissione dei reati di false comunicazioni alle autorità e di ostacolo alle funzioni di vigilanza, le attività soggette a vigilanza devono essere svolte in base a procedure aziendali contenenti la disciplina delle modalità e l'attribuzione di specifiche responsabilità in relazione:

- alle segnalazioni periodiche alle autorità previste da leggi e regolamenti;
- alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti;
- alla trasmissione di dati e documenti specificamente richiesti dalle Autorità di vigilanza;
- al comportamento da tenere nel corso degli accertamenti ispettivi.

I principi posti a fondamento di tali procedure sono:

- attuazione di tutti gli interventi di natura organizzativo-contabile necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni ed il loro puntuale invio all'Autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa applicabile;
- adeguata formalizzazione delle procedure in oggetto e successiva documentazione dell'esecuzione degli adempimenti in esse previsti, con particolare riferimento all'attività di elaborazione dei dati;
- nel corso dell'attività ispettiva, deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento degli accertamenti e non devono essere tenute condotte tali che siano di ostacolo all'esercizio delle funzioni di vigilanza (ad es. espressa opposizione, rifiuti ingiustificati,

ritardi nella trasmissione o nella consegna di documenti). In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di interloquire con l'autorità;

- alle ispezioni devono partecipare i soggetti a ciò espressamente delegati. L'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della Direzione aziendale di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali, che verranno conservati dall'Organismo di Vigilanza.

#### *Altre regole finalizzate alla prevenzione dei reati societari in genere*

A fianco delle regole di corporate governance e delle procedure esistenti, si dispone l'attuazione dei seguenti presidi integrativi:

- previsione di riunioni tra Collegio Sindacale e Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di corporate governance;
- trasmissione al Collegio Sindacale, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge;
- partecipazione dell'Organismo di Vigilanza alle riunioni assembleari mediante apposito invito predisposto dalla funzione Segreteria Generale. L'Organismo di Vigilanza valuterà l'utilità della propria partecipazione formalizzazione e/o aggiornamento di regolamenti interni e procedure aventi ad oggetto l'osservanza della normativa societaria.

#### **4.8. I controlli dell'Organismo di Vigilanza**

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Azienda.

L'Organismo di Vigilanza dovrà avere evidenza e mantenere traccia:

- di quanto posto in essere nella società al fine di fornire opportune indicazioni per la corretta redazione del bilancio;
- per quanto concerne il conferimento dell'incarico, l'Organismo di Vigilanza dovrà mantenere agli atti evidenza delle valutazioni circa le proposte, gli ambiti e le scelte effettuate da sottoporre al Consiglio di Amministrazione degli incarichi conferiti.

L'Organismo di Vigilanza dovrà, inoltre, esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.

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

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- monitorare sul rispetto delle procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

**5. – SEZIONE “C” – REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE COMMESSE CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICA**

**5.1. Introduzione e funzione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antinfortunistica**

**Termini relativi alle norme per la salvaguardia della salute e sicurezza sul lavoro**

<b>ASPP o Addetti al Servizio di Prevenzione e Protezione</b>	<i>I soggetti in possesso delle capacità e dei requisiti professionali di cui all'art. 32 del Decreto Sicurezza designati per l'espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione.</i>
<b>Cantiere Temporaneo o Mobile o Cantiere</b>	<i>Qualunque luogo in cui si effettuano lavori edili o di ingegneria civile così come individuati nell'allegato X del Decreto Sicurezza, ovvero, lavori di costruzione, manutenzione, riparazione, demolizione, conservazione, risanamento, ristrutturazione, equipaggiamento, trasformazione, rinnovamento o smantellamento di opere fisse, permanenti o temporanee, comprese le linee elettriche e le parti strutturali degli impianti elettrici. Sono, inoltre, lavori di costruzione edile o di ingegneria civile gli scavi ed il montaggio e lo smontaggio di elementi prefabbricati utilizzati per i lavori edili o di ingegneria civile.</i>
<b>Committente</b>	<i>Il soggetto per conto del quale viene realizzata l'intera opera edile o di ingegneria civile, indipendentemente da eventuali frazionamenti della sua realizzazione secondo quanto disposto dagli artt. 88 e ss. del Decreto Sicurezza.</i>
<b>Coordinatore per l'Esecuzione dei Lavori</b>	<i>Il soggetto incaricato dal committente o dal responsabile dei lavori tra l'altro, di verificare, con opportune azioni di coordinamento e controllo, l'applicazione, da parte delle imprese esecutrici e dei lavoratori, anche autonomi, delle disposizioni loro pertinenti contenute nel piano di sicurezza e coordinamento e di verificare altresì l'idoneità del piano operativo di sicurezza, assicurandone la coerenza con il primo.</i>
<b>Coordinatore per la Progettazione</b>	<i>Il soggetto, incaricato dal committente o dal responsabile dei Lavori, di redigere il piano di sicurezza e di coordinamento e di predisporre un fascicolo contenente le informazioni utili ai fini della prevenzione e della protezione dai rischi cui sono esposti i lavoratori.</i>
<b>Datore di Lavoro</b>	<i>Il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva in quanto titolare dei poteri decisionali e di spesa. È responsabile di provvedere all'attuazione di tutti gli obblighi fissati dal D.Lgs. 81/08 s.m.i. Gli obblighi non delegabili sono i seguenti:</i> <ul style="list-style-type: none"> <li>– La valutazione di tutti i rischi e la conseguente elaborazione del documento (Art. 28 Del D.Lgs. 81/08)</li> <li>– La designazione del responsabile del servizio di prevenzione e protezione dei rischi</li> </ul>
<b>Decreto Sicurezza</b>	<i>Il Decreto Legislativo 9 Aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e sicurezza nei luoghi di lavoro"</i>
<b>Dirigente</b>	<i>Il soggetto che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando sulla stessa</i>
<b>DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze</b>	<i>Il documento redatto dal datore di lavoro committente contenente una valutazione dei rischi che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze nei contratti di appalto, d'opera o di somministrazione ai sensi dell'art. 26 del Decreto Sicurezza</i>
<b>DVR o Documento di Valutazione dei Rischi</b>	<i>Il documento redatto dal datore di lavoro contenente una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale conseguente a tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, l'indicazione del nominativo del RSPP, del RLS e del medico competente che abbia partecipato alla valutazione del rischio, nonché l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione</i>
<b>Fascicolo dell'Opera</b>	<i>Il fascicolo predisposto a cura del coordinatore per la progettazione, eventualmente modificato nella fase esecutiva in funzione dell'evoluzione dei lavori ed aggiornato a cura del committente a seguito delle modifiche intervenute in un'opera nel corso della sua esistenza, contenente le informazioni utili ai fini della prevenzione e della protezione dei rischi cui sono esposti i lavoratori</i>
<b>Lavoratori</b>	<i>Soggetti che svolgono un'attività lavorativa nell'ambito della struttura organizzativa della società e contribuiscono, insieme al datore di lavoro, ai dirigenti ed ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro</i>
<b>Medico Competente</b>	<i>Il medico preposto all'attività di sorveglianza sanitaria. Il medico deve inoltre possedere uno dei titoli e dei requisiti formali e professionali indicati nel decreto sicurezza che collabora con il datore di lavoro, secondo quanto previsto all'Art.29 del D.Lgs.81/08 e s.m.i, ai fini della valutazione dei rischi e al fine di effettuare la sorveglianza sanitaria (di cui all'Art. 41 del D.Lgs 81/08 e s.m.i.) ed adempiere tutti gli altri compiti di cui al decreto sicurezza</i>
<b>Preposto</b>	<i>Il soggetto che in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa</i>
<b>Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro</b>	<i>I reati di cui all'Art. 25-septies del D.Lgs. 231/2001, ovvero l'omicidio colposo (Art. 589 c.p.) e le lesioni personali colpose gravi o gravissime (Art. 590 terzo comma c.p.) commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro</i>

<b>RLS o Rappresentante dei Lavoratori per la Sicurezza</b>	<i>Soggetto eletto o designato per rappresentare i lavoratori in relazione agli aspetti della salute e sicurezza sul lavoro</i>
<b>RSPP o Responsabile del Servizio di Prevenzione e Protezione</b>	<i>Il soggetto responsabile del servizio di prevenzione e protezione nominato dal datore di lavoro a cui risponde secondo quanto previsto dall'Art. 33 del D.Lgs. 81/08 e s.m.i.</i>
<b>Responsabile dei Lavori</b>	<i>Il soggetto che può essere incaricato dal committente ai fini della progettazione, dell'esecuzione o del controllo dell'esecuzione dell'opera o di una parte della procedura</i>
<b>Sorveglianza Sanitaria</b>	<i>L'insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori in relazione all'ambiente di lavoro, ai fattori di rischio professionali, ed alle modalità di svolgimento dell'attività lavorativa</i>
<b>SPP o Servizio di Prevenzione e Protezione</b>	<i>L'insieme delle persone, sistemi e mezzi esterni o interni alla società finalizzati all'attività di prevenzione e protezione dei rischi professionali</i>
<b>SLL</b>	<i>Salute e sicurezza dei lavoratori</i>
<b>Addetto al Primo Soccorso e addetto alla prevenzione incendi</b>	<i>Soggetti incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza</i>
<b>Referente Tecnico</b>	<i>Soggetto incaricato di assicurare la corretta realizzazione, in conformità alle norme e specifiche tecniche di progetto o del capitolato speciale, delle opere e dei servizi commissionati ad appaltatori/fornitori</i>

## 5.2. Criteri per la definizione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antinfortunistiche

I reati contro la persona sono ipotesi aggravate dei delitti di omicidio colposo e lesioni personali colpose. Tale aggravante consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro, sussiste non soltanto quando sia contestata la violazione di specifiche norme per la prevenzione degli infortuni sul lavoro, ma anche quando la contestazione ha per oggetto l'omissione dell'adozione di misure e/o accorgimenti per la più efficace tutela dell'integrità fisica dei lavoratori e, più in generale, la violazione di tutte le norme che, direttamente o indirettamente, tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui deve svolgersi.

## 5.3. Le fattispecie di reato richiamate dal D.Lgs 231/01

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'Art. 25-septies del Decreto.

Tale articolo, originariamente introdotto dalla Legge 3 Agosto 2007 n. 123, e successivamente sostituito ai sensi dell'art. 300 del Decreto Sicurezza, prevede l'applicazione di sanzioni pecuniarie ed interdittive agli Enti i cui esponenti commettano i reati di cui agli art. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Le fattispecie delittuose inserite all'art. 25-septies riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa della inosservanza delle norme per la prevenzione degli infortuni sul lavoro.

Il Consiglio dei Ministri in data 1 Aprile 2008 ha approvato il D.Lgs. 81/08 attuativo della delega di cui all'Art. 1 della L. 3 Agosto 2007 n. 123 in materia della salute e sicurezza nei luoghi di lavoro modificato dal D.Lgs. 3 Agosto 2009 n. 106 "Disposizioni integrative e correttive del D.Lgs 81/08".

### 5.3.1. Omicidio Colposo (art. 589 c.p.)

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa la morte di una persona".

I soggetti che possono rispondere del reato sono tutti i soggetti tenuti ad osservare o far osservare le norme di prevenzione o protezione, vale a dire i datori di lavoro, i dirigenti, i preposti, i soggetti destinatari delle deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro nonché i medesimi lavoratori.

La colpa, nel caso che ci interessa, consiste nell'aver il soggetto agito in violazione delle norme sulla prevenzione degli infortuni sul lavoro o meglio nella mancata adozione delle misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili alla luce dell'esperienza e delle più avanzate conoscenze tecnico scientifiche.

Se il reato in oggetto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena è della reclusione da due a sette anni.

Le misure di sicurezza vanno intese sia in senso statico vale a dire quale obbligo di adottare le misure di protezione e sicurezza oggettiva, sia in senso dinamico da intendersi come obbligo di formare ed informare i lavoratori circa i rischi propri dell'attività lavorativa nonché sulle misure idonee per evitare i rischi o ridurli al minimo.

La colpa per violazione delle norme per la prevenzione degli infortuni sul lavoro, pertanto, può essere ravvisata non solo in caso di violazione delle specifiche norme per la prevenzione degli infortuni sul lavoro ma anche nel caso in cui l'evento (che in caso di omicidio consiste nella morte) dipenda dall'omessa adozione di quelle misure ed accorgimenti imposti all'imprenditore ai fini della tutela dell'integrità fisica e della personalità del lavoratore da differenziare a seconda della tipologia di lavoro e tenendo conto della tecnica e dell'esperienza (art. 2087 del codice civile).

L'ente risponde, ai sensi del D.Lgs. 231/2001, qualora abbia tratto un vantaggio dall'evento dannoso che può consistere, ad esempio, in un risparmio di costi o di tempi per non aver adottato le misure di prevenzione degli infortuni sul lavoro.

Il datore di lavoro risponde, ad esempio, di omicidio colposo nel caso in cui la morte sia derivata dall'inosservanza delle norme sulla prevenzione degli infortuni sul lavoro qualora l'evento della morte si sia verificato nei confronti di un dipendente oppure di un soggetto estraneo all'ambiente di lavoro purché la presenza sul luogo di lavoro non sia eccezionale o atipica.

### **5.3.2. Lesioni personali colpose gravi e gravissime (art. 589 c.p.)**

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa una lesione personale".

La colpa richiesta dall'art. 25-septies del D.Lgs. 231/2001, consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro e di igiene e sicurezza. L'ente, risponde ai sensi del D.Lgs. 231/2001 sia per le ipotesi di lesioni gravi che per i casi di lesioni gravissime qualora abbia tratto un vantaggio concreto da intendersi, ad esempio, come già si è detto, quale una riduzione dei costi per approntare le misure di sicurezza richieste dalla normativa vigente o, comunque, dovute in considerazione delle nuove acquisizioni tecnologiche.

Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relativi all'igiene del lavoro o che abbiamo determinato una malattia professionale, è perseguibile d'ufficio.

Se il reato è commesso con violazione delle norme 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 500 Euro a 2.000 Euro e la pena per le lesioni gravissime è della reclusione da uno a tre 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.

Ai sensi del comma 1 dell'art. 583 cod. penale, la lesione è considerata **grave** nei seguenti casi:

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

Ai sensi del comma 2 dell'art. 583 cod. penale, la lesione è considerata invece **gravissima** se dal fatto deriva:

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

### **Esclusione della responsabilità amministrativa della società**

Come già indicato nella Parte Generale del Modello, il D.Lgs. n. 81/2008, all'art. 30, ha indicato le caratteristiche e i requisiti che deve possedere un modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto.

Pertanto nella predisposizione del Modello e nella definizione degli standard di controllo la società ha tenuto conto:

- Delle previsioni del Decreto
- Della vigente disciplina legislativa della prevenzione dei rischi lavorativi
- Del British Standard OHSAS 18001:2007 e/o UNI EN ISO 45001
- Delle Linee Guida Confindustria
- Dell'art. 30 del D.Lgs. 81/2008.

#### **5.4. Le Sanzioni previste dal Decreto**

Per entrambe le fattispecie delittuose sopra indicate - ossia omicidio colposo e lesioni personali colpose gravi o gravissime - gli enti sono soggetti ad una sanzione pecuniaria fino a 1000 quote (si consideri a tal riguardo che il valore di ogni quota può essere determinato, sulla base delle condizioni economiche e patrimoniali dell'ente, tra un minimo di 258 e un massimo di 1549 euro).

Perché si venga a configurare la responsabilità amministrativa della società ai sensi del Decreto, l'art. 5 del Decreto medesimo esige però che i reati siano stati commessi nel suo interesse o a suo vantaggio (ad esempio in termini di risparmi di costi per la salute e sicurezza sul lavoro).

Nel caso di condanna per uno dei reati sopra indicati, la società potrebbe essere assoggettata anche ad una sanzione interdittiva per una durata non inferiore a tre mesi e non superiore ad un anno.

Tali sanzioni interdittive possono consistere in:

- Interdizione dall'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 o sussidi ed eventuale revoca di quelli già concessi;
- Divieto di pubblicizzare beni o servizi.

#### **5.5. Le attività sensibili relative ai reati di omicidio colposo e lesioni colpose commesse**

Le principali aree aziendali a potenziale rischio reato relativamente alle fattispecie di cui all'art.25-septies del D.Lgs. 231/01 sono identificate e valutate nell'ambito dei documenti aziendali di valutazione dei rischi, predisposti ai sensi della normativa di riferimento e costantemente aggiornati in relazione all'evoluzione delle caratteristiche dell'attività produttiva.

Tuttavia, come precisato dalle Linee Guida di Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01, non è possibile individuare e limitare a priori alcun ambito di attività, dal momento che tale casistica di reati può, di fatto, investire la totalità delle componenti aziendali.

In altri termini, i reati oggetto della presente Parte Speciale potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Poiché la valutazione dei rischi rappresenta l'adempimento cardine per la garanzia della salute e della sicurezza dei lavoratori e poiché costituisce il principale strumento per procedere all'individuazione delle misure di tutela, siano esse la riduzione o l'eliminazione del rischio, l'operazione di individuazione e di rilevazione dei rischi deve essere effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza.

Il Modello, pertanto, prevede un costante aggiornamento del Documento di Valutazione dei Rischi (DVR), fornendo così evidenza del suo continuo adeguamento e della sua completezza.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella parte speciale del presente Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree di operatività ritenute più specificamente a rischio per la società risultano essere, ai fini della presente Parte Speciale del Modello, le seguenti:

- Attività di ufficio svolta dal personale dipendente, in particolare per ciò che concerne l'utilizzo di videoterminali;
- Attività di erogazione del servizio svolta dal personale dipendente, in particolare per ciò che concerne l'utilizzo di macchinari ed impianti presso i luoghi del Cliente ove viene erogato il servizio;
- Attività svolta da personale esterno presso la sede della società o sedi del Cliente, quali fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione (di cui all'art. 26 del Decreto Sicurezza).

Nell'ambito delle suddette aree di operatività, in virtù della probabilità che in tali contesti l'inosservanza delle norme poste a tutela della salute e sicurezza sul lavoro possa determinare uno degli eventi dannosi di cui all'art. 25 septies, sono state individuate le seguenti attività sensibili:

- Determinazione delle procedure interne in tema di salute e sicurezza sul lavoro volte a definire i compiti e le responsabilità in materia di sicurezza e a garantire una corretta gestione di tutti gli adempimenti posti in capo a ciascun destinatario così come disposti dal Decreto Sicurezza e dalla normativa primaria e secondaria ad esso collegata;
- Attribuzione di responsabilità in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
  - Attribuzioni di compiti e doveri in capo a ciascun Destinatario

- Attività del Servizio Prevenzione e Protezione e del Medico Competente
- Individuazione dei pericoli all'interno della sede e dei cantieri presso le sedi del Cliente ove viene erogato il servizio e valutazione dei rischi, con particolare riferimento a:
  - Stesura del Documento di Valutazione dei Rischi (DVR)
  - Valutazione dei rischi delle interferenze
  - Gestione dei contratti di appalto
- Sensibilizzazione di tutti i soggetti che, a diversi livelli, operano nell'ambito della struttura aziendale attraverso un'adeguata attività di informazione e la programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro
- Attuazione di adeguate attività di monitoraggio, verifica ed ispezione, in particolare per ciò che concerne:
  - L'aggiornamento delle misure in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza sul lavoro
  - La gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, attraverso l'eventuale irrogazione di provvedimenti disciplinari.

## 5.6. Organi e funzioni aziendali coinvolte

In relazione alle descritte attività sensibili, si ritengono particolarmente coinvolti alcuni organi e ruoli aziendali che ricoprono determinate funzioni aziendali.

### Amministrazione del Personale e Politiche Sindacali

In relazione all'attività di gestione dei Dipendenti relativamente ad eventuali provvedimenti disciplinari ed agli adempimenti infortunistici.

### Servizio Personale, Organizzazione e Formazione

Per attività di gestione dei dipendenti, di informazione e programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro.

### Consiglio di Amministrazione

Con riferimento all'approvazione del budget annuale di spesa in particolare per ciò che concerne i costi per la sicurezza. In qualità di Datore di Lavoro della società secondo la definizione di cui al Decreto Sicurezza, in relazione all'adempimento di tutti i compiti non delegabili a lui attribuiti dal suddetto decreto (e dunque, a titolo esemplificativo, attività di valutazione dei rischi e predisposizione del relativo Documento di Valutazione dei Rischi o valutazione dei rischi delle interferenze), nonché in merito all'inibizione dei comportamenti posti in violazione delle norme a tutela della salute e sicurezza dei Lavoratori attraverso l'adozione di eventuali provvedimenti disciplinari.

### Gestione Tecnica e Immobili

In quanto delegato dal datore di lavoro, in relazione all'adempimento di tutti i compiti da quest'ultimo delegabili (e dunque, a titolo esemplificativo, adempimento degli obblighi di informazione e formazione in tema di salute e sicurezza nei luoghi di lavoro, designazione dei Lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di primo soccorso e comunque di gestione delle emergenze, aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza sul lavoro, etc.,).

### Lavoratori e Preposti

In particolare con riferimento ai soggetti incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei luoghi di lavoro in caso di pericolo, di salvataggio, di primo soccorso e di gestione delle emergenze e, in generale, con riferimento a tutti, in merito all'osservanza delle norme poste a tutela dell'incolumità propria e altrui.

## 5.7. Principi e norme generali di comportamento

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Soggetti Apicali o in Posizione Apicale, dipendenti, collaboratori, fornitori della società nonché, nella misura in cui non rientrino in queste definizioni, dalle figure rilevanti di cui al successivo paragrafo (destinatari).

Obiettivo della presente Parte Speciale è che tutti i destinatari si attengano – in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della società – a regole di condotta conformi a quanto prescritto nella medesima Parte Speciale al fine di prevenire e impedire il verificarsi dei Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori, così come individuati dal Decreto Sicurezza, si prevede quanto segue:

- La gestione della tutela della salute e sicurezza sul lavoro (SSL) costituisce parte integrante della gestione aziendale
- La Azienda adotta un sistema di gestione della salute e sicurezza sul lavoro (SGSL) conforme all'art. 30 del D.Lgs 81/2008 ed ispirato al British Standard OHSAS 18001:2007 e/o ISO 45001.

Nel SGSL vengono definite le modalità per individuare, all'interno della struttura organizzativa aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme vigenti sulla salute e sicurezza dei lavoratori.

Esso integra obiettivi e politiche per la salute e sicurezza, nella gestione di sistemi di lavoro.

Adottando il SGSL, la Società si propone di:

- Contribuire a migliorare i livelli di salute e sicurezza sul lavoro;
- Ridurre incidenti ed infortuni, prevenire le potenziali malattie correlate al lavoro ed i rischi cui possono essere esposti i lavoratori o i terzi (clienti, fornitori, visitatori, etc.,);
- Aumentare la propria efficienza e le proprie prestazioni.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del Modello.

In generale, il sistema di organizzazione, gestione e controllo della Azienda deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività e in generale, delle proprie funzioni, gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- Leggi e regolamenti in tema di salute e sicurezza negli ambienti di lavoro;
- Il Codice Etico;
- Il presente Modello;
- Le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti la struttura organizzativa e il sistema di gestione della salute e sicurezza sul lavoro (SGSL).

La Azienda deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- Conoscibilità all'interno della società;
- Delimitazione dei ruoli, con una descrizione dei compiti di ciascuna funzione e dei relativi poteri;
- Descrizione delle linee di riporto.

Nello specifico, la Azienda, è dotata di una struttura organizzativa in conformità a quella prevista dalla normativa prevenzionistica vigente.

In coerenza con lo schema organizzativo e funzionale della Azienda sono stati definiti i compiti e le responsabilità in materia di SSL a partire dal Datore di Lavoro fino al lavoratore.

La Azienda ha, inoltre, individuato il Responsabile Sistema di Gestione (RSGSL), avente la responsabilità di mantenere operativo e far applicare il SGSL, riferendo direttamente al Datore di lavoro in merito alle prestazioni del sistema.

La Azienda, come previsto dal D.Lgs.81/08 e s.m.i, deve garantire il rispetto delle normative in tema di tutela della SSL, di tutela dell'ambiente nonché assicurare in generale un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività, anche attraverso:

- Una continua analisi del rischio e della criticità dei processi e delle risorse da proteggere;
- La programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione le condizioni lavorative e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro;
- Il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro;
- L'eliminazione/riduzione al minimo dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte;

- La sostituzione di ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso;
- Il controllo e l'aggiornamento delle metodologie di lavoro;
- Il controllo sanitario dei lavoratori, con particolare riguardo ai rischi specifici;
- Attività di informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, dei dirigenti e dei preposti sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro;
- La partecipazione e consultazione dei lavoratori e dei loro rappresentanti;
- La programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione del Codice Etico e di buone prassi;
- La formalizzazione di istruzioni adeguate ai lavoratori;
- L'uso di segnali di avvertimento e sicurezza;
- La regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti;
- La definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato.

Le misure relative alla SSL non devono in nessun caso comportare oneri finanziari per i lavoratori.

Nella scelta dei fornitori di beni o servizi, ivi inclusi in materia di SSL, devono essere privilegiati l'affidabilità del fornitore e la sua capacità di assolvere correttamente alle obbligazioni assunte, oltre al rapporto qualità/prezzo del bene o della prestazione offerta.

E' fatto espresso divieto di:

- Modificare o disattivare, senza autorizzazione i dispositivi di protezione individuali o collettivi;
- Modificare o togliere, senza autorizzazione, i dispositivi di sicurezza o di segnalazione o di controllo;
- Fabbricare, acquistare, noleggiare e utilizzare impianti, macchine, attrezzature o altri mezzi tecnici, inclusi dispositivi di protezione individuali e collettivi, non adeguati o non rispondenti alle disposizioni vigenti in materia di sicurezza;
- Accedere ad aree di lavoro a cui non si è autorizzati;
- Svolgere di propria iniziativa operazioni che non siano di competenza o che possano compromettere la sicurezza propria o di altri lavoratori.

### **5.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili**

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, etc.) gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Azienda, nello svolgimento delle attività sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25 septies, al rispetto della normativa vigente, delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio.

Tali regole e procedure sono contenute in una struttura documentale articolata in:

- Manuale del SGSL
- Documenti del SGSL (Politica, Obiettivi e Programma di Miglioramento, Organigramma, etc.,)
- Procedure del SGSL
- Istruzioni di lavoro
- Registrazioni relative agli aspetti inerenti la SSL tra le quali i registri di dati specifici
- La formazione, i risultati dei monitoraggi ed i risultati dei riesami
- Altri documenti (legislazione, norme tecniche, etc.,)

Il manuale del SGSL, in particolare, ha lo scopo di illustrare gli elementi fondamentali del sistema di gestione della sicurezza sul lavoro della Azienda.

In particolare intende descrivere le interazioni della Politica e degli obiettivi in materia di sicurezza sul lavoro fornendo anche un orientamento in merito alla documentazione del sistema stesso.

La Azienda, nella predisposizione del manuale e delle procedure in materia di SSL, rivolge particolare attenzione all'esigenza di garantire il rispetto dei seguenti principi:

- Devono essere formalmente identificate e documentate le responsabilità in materia di SSL, attraverso disposizioni organizzative e deleghe specifiche rilasciate da parte dei soggetti competenti e comunicate ai terzi interessati.
- Deve essere nominato il Medico Competente, devono, altresì, essere definiti appositi ed adeguati flussi informativi verso il Medico Competente in relazione ai processi ed ai rischi connessi all'attività produttiva.

- Devono essere tempestivamente identificati e valutati dal Datore di Lavoro i rischi per la SSL ivi compresi quelli riguardanti i lavoratori esposti a rischi particolari, deve, inoltre, essere tenuta in adeguata considerazione la struttura aziendale, la natura dell'attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, i macchinari, le attrezzature e gli impianti impiegati nelle attività e nei relativi cicli di protezione. La valutazione dei rischi deve essere documentata attraverso l'elaborazione, ai sensi della normativa prevenzionistica vigente, di un DVR che contenga quanto prescritto all'Art. 28 del D.Lgs. 81/08 e succ. mod.
- Il DVR deve essere elaborato dal DDL in collaborazione con il RSPP e il medico competente. Il DVR deve essere custodito presso il sito di riferimento ed aggiornato periodicamente e comunque in occasione di modifiche dell'organizzazione del lavoro significative ai fini della salute e sicurezza dei lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità. A seguito di tale rielaborazione, le misure di prevenzione debbono essere aggiornate.
- La valutazione del rischio deve essere condotta sviluppando il criterio di analisi dei rischi per singola fonte, identificata dalle norme di legge o ragionevolmente prevedibile, individuando nel documento di metodica le modalità di esecuzione. Il documento di metodica è quindi il punto di riferimento per la rappresentazione della metodologica di tutti i rischi, a cui fanno riferimento:
  - Le schede di valutazione del rischio specifica per mansione, sulla base del processo lavorativo e dell'organizzazione presente, atte ad evidenziare i rischi presenti per singole fasi o gruppi di fasi lavorative, e le misure tecniche, organizzative e formative messe in atto per la loro prevenzione;
  - Le relazioni tecniche, redatte a supporto dei rischi di mansione, atte a valutare o i rischi presenti nei vari ambienti riferibili alla generalità dei presenti (ad es. rischio incidente rilevante, etc.,) o rischi specifici e ben definiti ma relativi ad un esiguo numero di mansioni.
- Ai fini della gestione delle emergenze, della prevenzione degli incendi e dell'evacuazione dei lavoratori, nonché per il caso di pericolo grave e immediato, devono essere adottate adeguate misure, che prevedano:
  - Lo svolgimento e la documentazione di periodiche prove di evacuazione ossia delle simulazioni ove vengono provate le interazioni fra le varie strutture aziendali preposte, le modalità di evacuazione, le modalità di comunicazione, etc.,
  - La definizione e adozione di adeguate misure per il controllo di situazioni di rischio in caso di emergenza, con particolare riferimento all'elaborazione e periodico aggiornamento, a cura del Servizio di Protezione e Prevenzione, del Piano di sicurezza e di gestione dell'emergenza, testato periodicamente,
  - L'identificazione di lavoratori incaricati dell'attuazione delle misure di primo soccorso, gestione delle emergenze e antincendio che intervengono in funzione dell'area oggetto dell'emergenza,
  - La programmazione delle verifiche e delle manutenzioni relative alle apparecchiature antincendio e la regolare tenuta del Registro dell'Antincendio.
- Devono essere organizzati i necessari rapporti con i servizi pubblici competenti in materia di pronto soccorso, salvataggio, lotta antincendio e gestione delle emergenze.
- A seguito della valutazione dei rischi e secondo il programma di sorveglianza sanitaria devono essere individuate, in collaborazione con il medico competente ed SPP, le mansioni che necessitano di sorveglianza sanitaria periodica, con riferimento ai requisiti espressamente stabiliti dalla legge, ovvero risultanti da altri criteri/metodologie disponibili.
- Gli infortuni sul lavoro che comportano un'assenza di almeno un giorno devono essere tempestivamente, accuratamente e cronologicamente annotati in apposito registro o altra documentazione, redatta conformemente al modello approvato con Decreto del Ministero del Lavoro.
- Devono essere predisposte apposite procedure interne volte a definire le modalità ed i termini per l'acquisizione e la trasmissione dei dati informativi relativi agli infortuni sul lavoro.
- Deve essere definito, documentato, monitorato e periodicamente aggiornato, un programma di informazione dei lavoratori in materia di salute e sicurezza sul lavoro. Gli argomenti dell'informazione sono definiti anche in base alle risultanze della valutazione dei rischi e riguardano almeno:
  - I rischi per la salute e sicurezza connessi all'attività della Azienda in generale;
  - Le misure e le attività di protezione e prevenzione adottate;
  - I rischi specifici cui il lavoratore è esposto in relazione all'attività svolta, le normative di sicurezza e le disposizioni aziendali in materia;
  - Le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori;
  - I nominativi del responsabile del servizio di prevenzione e protezione e del medico competente;

- I nominativi dei lavoratori incaricati di applicare le misure lotta all'incendio, evacuazione dei lavoratori e pronto soccorso.

A ciascun lavoratore è inoltre fornita, per quanto di competenza, l'informazione specifica per quanto riguarda:

- Uso delle attrezzature di lavoro
  - Uso dei dispositivi di protezione individuale
  - Movimentazione manuale dei carichi
  - Utilizzo di VDT
  - Segnaletica visuale, gestuale, vocale, luminosa e sonora
  - Ogni altro fattore di rischio e argomento rilevante ai fini della SSL individuato e definito nel programma di informazione
- Deve essere redatto, documentato, implementato, monitorato ed aggiornato un programma di formazione ed addestramento periodico, con particolare riguardo ai lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione in materia di SSL. La formazione e l'addestramento devono essere differenziati in base al posto di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie. Devono essere monitorati ed adeguatamente documentati il regolare svolgimento e la partecipazione ai corsi di in materia di SSL.
- Deve essere attuato il coinvolgimento di tutti i lavoratori sui temi della SSL con continuità e periodicità.
- L'efficacia e l'adeguatezza delle misure di prevenzione e protezione devono essere periodicamente monitorate. Tali misure devono essere sostituite, modificate o aggiornate qualora ne sia riscontrata l'inefficacia e/o l'inadeguatezza, ovvero in relazione ad eventuali mutamenti organizzativi e dei rischi. E' necessario predisporre un piano di esecuzione delle verifiche, che indichi anche le modalità di esecuzione delle stesse, nonché le modalità di segnalazione di eventuali difformità.
- Il corretto utilizzo, da parte dei lavoratori, dei dispositivi di protezione individuale per lo svolgimento delle mansioni loro attribuite deve essere costantemente monitorato.
- Il DDL e il RSPP con la partecipazione del Medico competente, devono programmare ed effettuare apposite riunioni con i RLS, volte ad approfondire le questioni connesse alla prevenzione ed alla protezione dai rischi. Le riunioni devono essere adeguatamente formalizzate mediante la redazione di apposito verbale, il quale dovrà essere inviato all'Organismo di Vigilanza (ODV).
- Il divieto di fumare in tutti gli ambienti di lavoro deve essere formalizzato ed adeguatamente pubblicizzato.
- Deve essere garantita la manutenzione ordinaria e straordinaria dei dispositivi di sicurezza aziendale (ad esempio, porte tagliafuoco, lampade di emergenza, estintori, etc.). Manutenzioni ordinarie programmate devono essere effettuate sugli ambienti, gli impianti, i macchinari e le attrezzature generiche e specifiche in conformità alle indicazioni dei fabbricanti.
- Deve essere predisposto ed implementato un sistema di controllo interno idoneo a garantire la costante registrazione, anche attraverso l'eventuale redazione di apposita documentazione, delle verifiche svolte dalla Azienda in materia di SSL. In tale ambito, la Azienda deve prevedere che l'ODV effettui un'attività di monitoraggio periodica della funzionalità del complessivo sistema preventivo adottato. A tal fine deve essere inviata all'ODV copia della reportistica periodica in materia di SSL, del verbale della riunione periodica di cui all'art. 35 del D.Lgs. 81/08 e succ. mod, nonché tutti i dati relativi agli infortuni sul lavoro occorsi nei siti della Azienda.
- Devono essere previste nel sistema disciplinare e meccanismo sanzionatorio adottato dalla Azienda, nel rispetto di quanto previsto dalla legge e dalla contrattazione collettiva, apposite sanzioni per la violazione del Modello in materia di SSL.

La Azienda ha facoltà di integrare, in qualsiasi momento, i principi elencati nel presente paragrafo così come le procedure aziendali vigenti, qualora ritenuto opportuno al fine di garantire la SSL.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti, salvo l'obbligo in capo a tutti i destinatari di segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

#### **Il Datore di Lavoro**

Al datore di lavoro sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti non delegabili:

- Valutare tutti i rischi per la sicurezza e per la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di

lavoratori esposti a rischi particolari (es. rischi connessi alla differenza di genere, alla provenienza da altri Paesi, etc.,) anche nella scelta delle attrezzature di lavoro, nonché nella sistemazione dei luoghi di lavoro; a tal riguardo, nella scelte operate il Datore di Lavoro dovrà garantire il rispetto degli standard tecnico-strutturali previsti dalla legge;

- Elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi con data certa contenente:
  - Una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa;
  - L'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuale adottati, a seguito della suddetta valutazione dei rischi;
  - Il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
  - L'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
  - L'indicazione del nominativo del RSPP, degli RLS e del medico competente che abbiano partecipato alla valutazione del rischio;
  - L'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il RSPP e con il medico competente. La valutazione dei rischi è oggetto di consultazione preventiva con il RLS, e va nuovamente effettuata in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei Lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione, a seguito di infortuni significativi o quando i risultati della Sorveglianza Sanitaria ne evidenzino la necessità.

Nell'ambito della riunione annuale ai fini della sicurezza a cui partecipano il Datore di Lavoro, il RSPP, il Medico Competente, gli RLS viene riesaminato, tra gli altri documenti, anche il Documento di Valutazione dei Rischi.

- Designare il Responsabile del Servizio di Prevenzione e Protezione sia esso interno o esterno all'azienda.

Al Datore di Lavoro sono attribuiti i seguenti altri compiti dallo stesso delegabili a soggetti qualificati. Tali compiti, previsti dal Decreto Sicurezza, riguardano, tra l'altro, il potere di:

- Nominare il medico competente per l'effettuazione della sorveglianza sanitaria;
- Designare preventivamente i Lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione delle emergenze;
- Fornire ai Lavoratori i necessari ed idonei dispositivi di protezione individuale, sentito il RSPP ed il medico competente;
- Adottare le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
- Adempiere agli obblighi di informazione e formazione di cui ai successivi paragrafi;
- Comunicare all'INAIL, a fini statistici e informativi, i dati relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, le informazioni relative agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni;
- Convocare la riunione periodica di cui all'art. 35 del Decreto Sicurezza;
- Aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- Prevedere un adeguato sistema di vigilanza sul rispetto delle procedure e delle misure di sicurezza da parte dei lavoratori, individuando specifiche figure a ciò deputate;
- Adottare provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservino le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza;

In relazione a tali compiti, ed a ogni altro compito affidato al datore di lavoro che possa essere da questi delegato ai sensi del Decreto Sicurezza, la suddetta delega, cui deve essere data adeguata e tempestiva pubblicità, è ammessa

con i seguenti limiti e condizioni:

- Che essa risulti da atto scritto recante data certa;
- Che il delegato possieda tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- Che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- Che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
- Che la delega sia accettata dal delegato per iscritto.

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e partecipativo, il datore di lavoro fornisce al Servizio di Prevenzione e Protezione e al Medico Competente informazioni in merito a:

- La natura dei rischi;
- L'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
- La descrizione degli impianti e dei processi produttivi;
- I dati relativi agli infortuni e quelli relativi alle malattie professionali.

#### **Il Servizio di Prevenzione e Protezione**

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro organizza il Servizio di Prevenzione e Protezione all'interno dell'azienda o incarica persone o servizi esterni assicurandosi che gli ASPP ed i RSPP, da questi nominati, siano in possesso delle capacità e dei requisiti professionali di cui all'Art. 32 del Decreto Sicurezza (es. possesso di un titolo di studio di istruzione secondaria superiore, nonché di un attestato di frequenza, con verifica di apprendimento, a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro, etc., ).

Il SPP provvede a:

- Individuare i fattori di rischio, valutare i rischi e individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente e sulla base della specifica conoscenza dell'organizzazione aziendale;
- Elaborare, per quanto di competenza, le misure preventive e protettive di cui all'art. 28 del Decreto Sicurezza e dei sistemi di controllo di tali misure;
- Elaborare procedure di sicurezza per le varie attività aziendali;
- Proporre programmi di informazione e formazione dei lavoratori;
- Partecipare, attraverso il RSPP, alla "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza;
- Partecipare alle consultazioni in materia di tutela della salute e della sicurezza;
- Informare i lavoratori, a nome e per conto del Datore di Lavoro, sulle tematiche di cui all'art. 36 del Decreto Sicurezza come indicato nel dettaglio al successivo paragrafo;
- Segnalare all'Organismo di Vigilanza la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro.

L'eventuale sostituzione del RSPP deve essere comunicata all'Organismo di Vigilanza con l'espressa indicazione delle motivazioni a supporto di tale decisione.

#### **Il Medico Competente**

Il Medico Competente deve essere in possesso di uno dei titoli di cui all' art. 38 del Decreto Sicurezza e, precisamente:

- Specializzazione in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica;
- Docenza in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica, o in tossicologia industriale, o in igiene industriale, o in fisiologia ed igiene del lavoro o in clinica del lavoro;
- Autorizzazione di cui all'articolo 55 del D.Lgs. 277/91 e successive modifiche che prevede una comprovata esperienza professionale di almeno 4 anni.

Il Medico Competente provvede a:

- Collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla predisposizione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori;
- Effettuare le visite mediche preventive e periodiche previste dalla legge e da programmi di prevenzione opportunamente stabiliti;

- Fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informarli sui risultati;
- Esprimere il giudizio di idoneità specifica alla mansione;
- Istituire ed aggiornare, per ogni lavoratore sottoposto a sorveglianza sanitaria, le cartelle sanitarie e di rischio, con salvaguardia del segreto professionale;
- Visitare gli ambienti di lavoro, congiuntamente al RSPP, redigendo specifico verbale e partecipare alla programmazione del controllo dell'esposizione dei lavoratori;
- Comunicare, in occasione della "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza, i risultati anonimi collettivi degli accertamenti sanitari, fornendo le informazioni necessarie;
- Collaborare all'attività di informazione e formazione dei lavoratori;
- Collaborare con il Datore di Lavoro alla predisposizione del servizio di pronto soccorso.

Il Medico Competente può avvalersi, per accertamenti diagnostici, della collaborazione di medici specialisti scelti in accordo con il Datore di Lavoro che ne sopporta gli oneri.

Il Datore di Lavoro assicura al Medico Competente le condizioni necessarie per lo svolgimento di tutti i suoi compiti garantendone la piena autonomia.

#### **I Rappresentanti dei Lavoratori per la Sicurezza (RLS)**

Sono i soggetti eletti o designati, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro.

Gli RLS:

- Accedono ai luoghi di lavoro;
- Sono consultati preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- Sono consultati sulla designazione del RSPP, degli ASPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso;
- Sono consultati in merito all'organizzazione delle attività formative;
- Promuovono l'elaborazione, l'individuazione e l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei Lavoratori;
- Partecipano alla "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza;
- Ricevono informazioni e la documentazione aziendale inerenti alla valutazione dei rischi e le misure di prevenzione relative, nonché quelli inerenti alle sostanze e ai preparati pericolosi, alle macchine, agli impianti, all'organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali; ricevono altresì, su loro richiesta e per l'espletamento delle loro funzioni, copia del Documento di Valutazione dei Rischi;
- Ricevono informazioni provenienti dai servizi di vigilanza;
- Ricevono un'informazione adeguata e comunque non inferiore a quella prevista per i lavoratori ai sensi dell'art. 37 del Decreto Sicurezza;
- Formulano osservazioni in occasione di visite e verifiche effettuate dalle autorità competenti dalle quali siano sentiti;
- Avvertono il Datore di Lavoro dei rischi individuati nel corso della loro attività;
- Possono far ricorso alle autorità competenti qualora ritengano che le misure di prevenzione e protezione dai rischi adottate dal Datore di Lavoro o dai dirigenti ed i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.

Gli RLS dispongono del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi e degli spazi necessari per l'esercizio delle funzioni e delle facoltà loro riconosciute; non possono subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei loro confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

#### **I Lavoratori**

È cura di ciascun lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite.

I lavoratori devono:

- Osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai preposti, ai fini della

protezione collettiva ed individuale;

- Utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, nonché gli eventuali dispositivi di sicurezza;
- Segnalare immediatamente al Datore di Lavoro, al Dirigente o al Preposto le deficienze dei mezzi e dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al Rappresentante dei Lavoratori per la Sicurezza;
- Non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- Non compiere di propria iniziativa operazioni né manovre che non siano di loro competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori;
- Sottoporsi ai controlli sanitari previsti nei loro confronti;
- Contribuire, insieme al Datore di Lavoro, ai Dirigenti e ai Preposti, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

## 5.9. Attività di Informazione e Formazione

### **ATTIVITÀ DI INFORMAZIONE**

La Azienda è tenuta a fornire adeguata informazione ai dipendenti e nuovi assunti, ai lavoratori, agli stagisti circa:

- I rischi specifici dell'impresa;
- Le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle prescrizioni di legge e di autoregolamentazione di cui l'azienda si è dotata;
- Il ruolo e responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità delle prescrizioni di cui sopra;
- Le misure di prevenzione e protezione adottate nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del D.Lgs. 231/2001.

Tale informazione deve essere facilmente comprensibile per ciascun lavoratore, consentendo a ciascuno di acquisire le necessarie conoscenze e deve essere preceduta, qualora riguardi lavoratori immigrati, dalla verifica della comprensione della lingua utilizzata nel percorso formativo.

Ciò premesso, la Azienda, in considerazione dei diversi ruoli, responsabilità, capacità e dei rischi cui è esposto ciascun dipendente, fornisce tra l'altro, adeguata informazione ai lavoratori sulle seguenti tematiche:

- Sui rischi per la salute e sicurezza sul lavoro, connessi all'attività della Azienda in generale e su quelli specifici cui ciascun lavoratore è esposto in relazione all'attività svolta;
- Sulle misure di prevenzione e protezione adottate;
- Sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro;
- Sui nominativi dei lavoratori incaricati delle misure di emergenza e di pronto soccorso, nonché del Medico Competente.

Si precisa infine che nei confronti dei dipendenti distaccati se esistenti, in capo ai quali permangono gli obblighi in materia di prevenzione e protezione, la Azienda destina adeguata informativa circa i rischi generalmente connessi alle mansioni per le quali i dipendenti vengono distaccati.

La Azienda organizza altresì periodici incontri tra le funzioni preposte alla sicurezza sul lavoro fornendone comunicazione all'Organismo di Vigilanza.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione. A tali fini la Azienda deve mettere a disposizione dei destinatari una bacheca che conterrà i vari riferimenti in tema di sicurezza, la normativa, la descrizione della struttura, le circolari interne ed i nominativi degli RLS.

### **ATTIVITÀ DI FORMAZIONE**

La Azienda deve fornire adeguata formazione a tutti i lavoratori in materia di sicurezza sul lavoro e il contenuto della stessa deve essere facilmente comprensibile e consentire di acquisire le conoscenze e competenze necessarie.

A tal riguardo si specifica che:

- Il RSPP e il medico competente debbono partecipare alla stesura del piano di formazione;

- La formazione erogata deve prevedere questionari di valutazione dell'apprendimento;
  - La formazione deve essere adeguata ai rischi della mansione cui il lavoratore è in concreto assegnato;
  - I lavoratori che cambiano mansione e quelli trasferiti devono fruire di formazione specifica, preventiva e/o aggiuntiva, ove necessario, per il nuovo incarico;
  - Ciascun lavoratore deve essere sottoposto a tutte quelle azioni formative rese obbligatorie dalla legge, tra le quali, ad esempio:
    - L'uso delle attrezzature di lavoro
    - La movimentazione manuale carichi
    - L'uso dei videoterminali
    - La segnaletica visuale, gestuale, vocale, luminosa e sonora.
  - Gli addetti a specifici compiti in materia di emergenza devono ricevere specifica formazione;
  - La Azienda deve effettuare periodiche esercitazioni di emergenza di cui deve essere data evidenza (attraverso, ad esempio, la verbalizzazione dell'avvenuta esercitazione con riferimento alle modalità di svolgimento e alle risultanze);
  - I neo assunti - in assenza di pregressa esperienza professionale/lavorativa e di adeguata qualificazione - non possono essere adibiti in autonomia ad attività operativa ritenuta più a rischio infortuni se non dopo l'acquisizione di un grado di professionalità idoneo allo svolgimento della stessa mediante adeguata formazione non inferiore ad almeno tre mesi dall'assunzione, salvo periodi più ampi per l'acquisizione di qualifiche specifiche.
- Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione.

#### **5.10. Istituzione di flussi informativi**

Con l'obiettivo di rafforzare l'efficacia del sistema organizzativo adottato dalla Azienda per la gestione della salute e sicurezza dei Lavoratori e quindi per la prevenzione degli infortuni, la Azienda si organizza per assicurare un adeguato livello di circolazione e condivisione delle informazioni tra tutti i lavoratori.

In primo luogo, la Azienda mette a disposizione un apposito sistema di comunicazione aziendale attraverso cui ciascun Lavoratore ha la possibilità di conoscere le procedure aziendali in tema di sicurezza e portare a conoscenza del proprio superiore gerarchico le proprie osservazioni, proposte ed esigenze di miglioramento relative alla gestione della salute e sicurezza in ambito aziendale.

In secondo luogo, la Azienda garantisce a tutti i lavoratori un'adeguata e costante informativa attraverso la predisposizione di comunicati e l'organizzazione di incontri periodici, cui l'Organismo di Vigilanza ha la facoltà di partecipare, che abbiano ad oggetto:

- Eventuali nuovi rischi in materia di salute e sicurezza
- Modifiche nella struttura organizzativa per la gestione della salute e sicurezza nei luoghi di lavoro
- Predisposizione di nuove procedure o aggiornamento in merito a quelle esistenti per la gestione della salute e sicurezza sul lavoro
- Ogni altro aspetto inerente la salute e sicurezza dei lavoratori

#### **5.11. Conservazione della documentazione rilevante**

La Azienda garantisce che vengano adeguatamente conservati su supporto cartaceo ed informatico, e aggiornati i seguenti documenti:

- La cartella sanitaria, ove prevista, deve essere istituita e aggiornata dal medico competente e custodita dal Datore di Lavoro;
- Il registro / documentazione relativa agli infortuni;
- Verbalizzazione delle visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal medico competente;
- Documenti che registrano gli adempimenti espletati in materia di sicurezza e salute sul lavoro;
- Documento di Valutazione dei Rischi;
- Documento di Valutazione dei Rischi integrato ("DUVRI");
- Nomina formale del Responsabile e degli Addetti al Servizio di Prevenzione e Protezione (RSPP e ASPP), del Medico Competente, degli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, nonché degli eventuali Dirigenti e Preposti;
- Documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti alla realtà aziendale;
- Documentazione inerente a regolamenti ed accordi aziendali;

- Manuali di istruzione per l'uso di macchine e attrezzature forniti da fabbricanti e/o fornitori;
- Ogni procedura adottata dall'azienda per la gestione della salute e sicurezza sui luoghi di lavoro;
- Tutta la documentazione relativa alle attività di cui a "Informazione" e "Formazione", che deve essere conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza.

### **5.12. Contratto d'appalto**

La Azienda predispone e mantiene aggiornato l'elenco delle aziende che operano all'interno dei propri siti con contratto d'appalto.

Le modalità di gestione e di coordinamento dei lavori in appalto vengono formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti in capo al Datore di Lavoro di cui all'art. 26 del Decreto Sicurezza, tra cui, in via esemplificativa:

- Verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso:
  - Acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato;
  - Acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'articolo 4 del Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445;
- Fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- Cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- Coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori;
- Predisporre un unico DUVRI che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva; tale documento deve allegarsi al contratto di appalto o d'opera;
- Verificare in fase di gestione del contratto ed esecuzione dei lavori il rispetto delle misure previste di prevenzione e protezione e il rispetto degli adempimenti di legge verso il personale di cui al punto precedente;
- Assicurarsi che il personale dell'impresa appaltatrice o subappaltatrice esponga, in presenza dello specifico obbligo di legge, la tessera di riconoscimento con fotografia, dati anagrafici e indicazione del Datore di Lavoro.

Nei contratti di somministrazione, di appalto e di subappalto, vengono specificamente indicati i costi relativi alla sicurezza del lavoro.

A tali dati possono accedere, su richiesta, gli RLS e le organizzazioni sindacali dei lavoratori.

Infine, nei contratti di appalto viene chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

### **CLAUSOLE CONTRATTUALI**

La Azienda inserisce, nei contratti con i Collaboratori esterni e con i Partner, un'apposita dichiarazione dei medesimi con cui afferma:

- Di essere a conoscenza della normativa di cui al Decreto e delle sue implicazioni per la società, nonché dell'adozione da parte della stessa del Modello e del Codice Etico
- Di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Decreto
- Di impegnarsi al rispetto delle prescrizioni contenute nel Decreto, nonché dei principi contenuti nel Modello, nel Codice Etico

Inoltre, nei contratti con i collaboratori esterni e con i partner, viene inserita un'apposita clausola che regola le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché dei principi di cui al Modello (ad es. clausole risolutive espresse, penali).

### **PRINCIPI PROCEDURALI SPECIFICI**

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale i dipendenti sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- Organigramma aziendale;
- Documento di Valutazione dei Rischi con i relativi documenti integrativi;
- Procedure interne di selezione, qualificazione e monitoraggio dei fornitori di servizi;

- Procedure interne finalizzate a garantire il mantenimento di elevati standard di sicurezza nei lavori appaltati a terzi a tutela sia del personale dell'azienda che di quello delle ditte appaltatrici presso la sede aziendale;
- Procedure interne per l'informazione e la formazione del personale in materia di tutela della salute e della sicurezza sul lavoro;
- Codice Etico.

Tali procedure e i documenti devono essere considerati come parte integrante delle strutture di organizzazione gestione e controllo necessarie per il corretto funzionamento ed efficacia del Modello 231 e sono aggiornati dalle funzioni aziendali e dagli Organi Sociali competenti.

### **5.13. I Controlli dell'Organismo di Vigilanza**

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate in tema di sicurezza sul lavoro, la documentazione prevista dal Decreto Sicurezza, il rispetto delle relative formalità, nonché l'adeguatezza dei sistemi dei controlli interni adottati in tale ambito.

In particolare l'Organismo di Vigilanza dovrà esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Al fine di svolgere i propri compiti, l'Organismo di Vigilanza può:

- Partecipare agli incontri organizzati dalla Azienda tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- Accedere a tutta la documentazione di cui al precedente paragrafo.

La Azienda istituisce altresì a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda.

L'Organismo di Vigilanza si incontra regolarmente ed almeno semestralmente con il RSPP per una disamina complessiva degli aspetti relativi alle tematiche sulla sicurezza sul lavoro.

## **6. – SEZIONE “D” – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI**

### **6.1. Introduzione e funzione della parte speciale dei reati informatici e di trattamento illecito dei dati**

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Sociali aziendali, nonché dai suoi Collaboratori esterni e dai Partner come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i Dipendenti e gli altri soggetti eventualmente autorizzati adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi degli illeciti in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Dipendenti e gli altri soggetti eventualmente autorizzati sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all’Organismo di Vigilanza, nonché ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La Azienda adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti.

### **6.2. Criteri per la definizione dei reati informatici e di trattamento illecito dei dati**

Ad integrazione delle definizioni elencate nella Parte Generale del Modello, si consideri la seguente ulteriore definizione da applicare alla presente Parte Speciale:

**"Delitti Informatici"**: sono i delitti richiamati dall'art. 24-bis del Decreto e disciplinati dal codice penale agli artt. 491-bis, 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-quinquies.

### **6.3. Le fattispecie di reato richiamate dal D.Lgs 231/01**

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 delle società. L’art. 7 del predetto provvedimento ha introdotto nel Decreto l’art. 24 - bis “Delitti informatici e trattamento illecito di dati”, che riconduce la responsabilità amministrativa degli enti ai reati individuati nelle sezioni seguenti.

La presente Parte Speciale si riferisce ai Delitti informatici e trattamento illecito di dati (di seguito, per brevità, i “Delitti Informatici”).

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'art. 24-bis del D.Lgs. n. 231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi.

#### **6.3.1. Falsità in documenti informatici (art. 491-bis c.p.)**

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, lett. p), D.Lgs. 82/2005, salvo modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell’addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l’alterazione di informazioni a valenza probatoria presenti sui sistemi dell’ente, allo scopo di eliminare le prove di un altro reato.

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

Tale reato si realizza quando un soggetto, “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 di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o

istruzioni idonee al predetto scopo". Tale reato 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 il danno è commesso:

- 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;
- 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.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-quater, pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (ad esempio, badge, carte di credito, bancomat e smart card).

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet).

L'art. 615-quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente di una azienda autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'azienda oppure carisca in altro modo fraudolento o ingannevole il codice di accesso.

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

Questo reato si configura quando "il soggetto che presta servizi di certificazione di firma elettronica, 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". Tale reato è punito con la reclusione fino a tre anni e con la multa da Euro 51 a Euro 1.032.

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

### **6.4. Le attività sensibili relative ai reati informatici**

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

L'analisi dei processi ha consentito di individuare le seguenti "attività sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24 - bis del d.lgs. 231/2001:

- a) Gestione dei profili utente e del processo di autenticazione;
- b) Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio;
- c) Gestione e protezione della postazione di lavoro;
- d) Gestione degli accessi da e verso l'esterno;
- e) Gestione e protezione delle reti;
- f) Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD);
- g) Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.).

I delitti trovano come presupposto l'utilizzo della rete informatica intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e precisamente:

- Tutte le attività aziendali svolte dal personale tramite l'utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad Internet;

- Gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica;
- Erogazione di servizi di installazione e servizi professionali di supporto al personale (ad esempio, assistenza, manutenzione, gestione della rete, manutenzione e security).

### **6.5. Organi e funzioni aziendali coinvolte**

In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali

- **Servizio Infrastrutture/Servizio Sicurezza**

*In relazione alle Attività Sensibili queste due funzioni sono coinvolte per la gestione e la corretta dotazione di strumenti informatici ai dipendenti ed il controllo su tutto il sistema informatico aziendale.*

- **Consiglio di Amministrazione**

*I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili.*

- **Servizio Audit**

*Considerata la funzione non operativa dell'Internal Audit, questa, tuttavia, potrebbe presentare il rischio di culpa in vigilando, consistente nel mancato o non corretto controllo delle attività che possono essere considerate a rischio per la società.*

- **Servizio Personale e Organizzazione**

*In relazione ad Attività Sensibili di cui sopra questa funzione è coinvolta per i rapporti che intrattiene con tutti gli esponenti aziendali e con la formazione, informazione in merito all'utilizzo dei sistemi informatici della società.*

### **6.6. Principi e regole di comportamento**

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del Modello.

In generale, il sistema di organizzazione, gestione e controllo della Azienda deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte ed, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Azienda, devono conoscere e rispettare:

1. gli standard generali di controllo
2. i principi di comportamento individuati nel Codice Etico
3. quanto regolamentato dalla documentazione e dagli atti aziendali
4. le disposizioni di legge.

### **6.7. Principi e norme generali di comportamento**

La presente Parte Speciale è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a Rischio reato informatico e nello svolgimento delle attività sensibili precedentemente citate.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale ed al fine di perseguire la prevenzione dei Reati Informatici è fatto espresso divieto a tutti i Soggetti coinvolti di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 24-bis del D. Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale.

In generale, la prevenzione dei crimini informatici è svolta attraverso adeguate misure tecnologiche, organizzative e normative ed in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- Previsione nel Codice Etico di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno della società che tramite apparecchiature non soggette al controllo della stessa;
- Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite;

- Predisposizione di adeguati strumenti tecnologici atti a prevenire e/o impedire la realizzazione di reati informatici da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio;
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.

Conseguentemente, gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nelle svolgimento della attività a rischio hanno l'espresso obbligo di perseguire i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

- **Segregazione delle attività:**  
si richiede l'applicazione del principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio, tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso; ad esempio: progettazione ed esercizio, acquisto di beni e risorse e relativa contabilizzazione.
- **Esistenza di procedure:**  
devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività.
- **Poteri autorizzativi e di firma:**  
definire livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio
- **Tracciabilità:**  
tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio; ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione distruzione delle registrazioni effettuate.
- **Gestione delle segnalazioni:**  
raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati informatici rilevati da soggetti interni e esterni all'ente.
- **Ripporto all'OdV:**  
riferire prontamente all'OdV eventuali situazioni di irregolarità.

#### **6.8. Principi di riferimento e specifici relativi alla regolamentazione delle attività sensibili**

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nelle svolgimento delle attività a rischio sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 24-bis del D.Lgs. 231/01, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale attività a rischio.

Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area quali, ad esempio:

- **Esistenza di una normativa/procedura aziendale relativa a:**
  1. Gestione degli accessi che tra l'altro individua le seguenti fasi:
    - Attribuzione accessi;
    - Assegnazione dei codici identificativi personali (richieste di abilitazione/modifica delle utenze);
    - Disattivazione dei codici utente associati al personale che ha perso il diritto di accesso a tutti i sistemi informatici o che non accede più ai vari sistemi;
    - Attività di controllo volta a verificare, prima della creazione di un'utenza, che la stessa non sia già stata precedentemente assegnata/disabilitata/rimossa e che uno stesso codice identificativo personale non venga assegnato, neppure in tempi diversi, a persone diverse.
  2. Modalità di utilizzo e di salvaguardia del PC intese come misure che l'utente deve adottare per garantire un'adeguata Protezione delle apparecchiature incustodite.

3. Installazione di software sui sistemi operativi.
  4. Dismissione dei supporti di memorizzazione su cui sono registrate informazioni aziendali.
- Attuazione di un sistema di accesso logico idoneo a controllare che le attività di utilizzo delle risorse da parte dei processi e degli utenti e di accesso alla rete si esplicino attraverso la verifica e la gestione dei diritti d'accesso.
  - Presenza di sistemi di protezione antivirus e antispam.
  - Esistenza di una serie di procedure, in materia di “privacy” e di “security”, che disciplinano gli aspetti legati al corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni.
  - Attuazione del progetto di formazione, volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy.
  - Consegna a ciascun dipendente della Azienda, contestualmente all'assegnazione del pc e/o dell'indirizzo di posta internet di norme per l'utilizzo dei Personal Computer aziendali e sull'utilizzo della posta internet e in generale di documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico.
  - Individuazione tempestiva delle vulnerabilità dei sistemi.
  - Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che costituiscono il patrimonio della Azienda oggetto di protezione (risorse tecnologiche e informazioni), attraverso, l'adozione di sistemi antincendio, antiallagamento, di condizionamento, gruppi di continuità UPS e di regolamentazione degli accessi.
  - Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici (registrazione dei log on e log off).
  - Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking attraverso tra l'altro una serie di provvedimenti volti a garantire che:
    - L'informazione inserita ed elaborata dal sistema pubblico sia processata completamente e in modo tempestivo;
    - Le informazioni sensibili siano protette durante i processi di raccolta e di conservazione;
    - L'accesso al sistema pubblico non consenta ingressi fortuiti alle reti con cui è connesso.

#### **Principi procedurali specifici**

In particolare, si elencano qui di seguito le regole che devono essere rispettate dalla Azienda e dai dipendenti e dagli altri soggetti eventualmente autorizzati nell'ambito delle Attività Sensibili:

- i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati;
- è vietato introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato;
- è vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili effettuata dal Servizio Infrastrutture;
- è vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società;
- è vietato divulgare, cedere o condividere con personale interno o esterno alla Azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
- è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;

- è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- è vietato comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- è vietato lo spamming come pure ogni azione di risposta allo spam;
- è obbligatorio segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

La Azienda si impegna a porre in essere i seguenti adempimenti:

- informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi (cfr. Manuale utilizzo User ID e password);
- fare sottoscrivere ai dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali;
- informare i dipendenti e agli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso (cfr. Manuale utilizzo User ID e password);
- impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- fornire un accesso da e verso l'esterno (connessione alla rete Internet) esclusivamente ai sistemi informatici dei dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria;
- limitare gli accessi alla stanza server unicamente al personale autorizzato;
- proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- fornire ogni sistema informatico di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- impedire l'installazione e l'utilizzo di software non approvati dalla Azienda e non correlati con l'attività espletata per la stessa;
- limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file);
- impedire l'installazione e l'utilizzo, sui sistemi informatici della Azienda, di software (c.d. "P2P", di files sharing o di instant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.) senza alcuna possibilità di controllo da parte della società;
- qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna WiFi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;
- prevedere un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati (Cfr. Manuale utilizzo user Id e password);
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti e degli altri soggetti eventualmente autorizzati (i.e. connessione tramite VPN o RAS);
- effettuare periodicamente, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile, controlli ex ante ed ex post sulle attività effettuate dal personale sulle reti.

### **6.9. I controlli dell'Organismo di Vigilanza**

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'art. 24-bis del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 24-bis del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24-bis del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio di delitti informatici, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti informatici di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche;
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale;
- Monitorare il rispetto delle procedure e la documentazione interna (i.e. Normativa Aziendale e Modulistica) per la prevenzione dei Delitti Informatici in costante coordinamento con le funzioni Sicurezza Informatica ed Internal Audit;
- Consultarsi con il responsabile della Sicurezza Informatica e/o del Servizio Sistemi Informativi ed invitare periodicamente lo stesso a relazionare alle riunioni dell'OdV;
- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- Conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

## **7. – SEZIONE “E” – REATI AMBIENTALI**

### **7.1. Introduzione e funzione della parte speciale dei reati ambientali**

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Sociali dell'azienda, nonché dai suoi Collaboratori esterni e dai suoi Partner come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i Destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi degli illeciti in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai Responsabili delle altre funzioni della società, che cooperano con tale organismo, gli strumenti esecutivi necessari affinché gli stessi possano esercitare le attività di controllo, monitoraggio e verifica.

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti.

### **7.2. Criteri per la definizione dei reati ambientali**

Il Consiglio dei Ministri n. 145 del 7 luglio 2011 ha approvato, in via definitiva, il Decreto Legislativo n. 121/2011, attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della Direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni, estendendo la responsabilità amministrativa degli enti ad alcuni illeciti commessi in violazione delle norme a tutela dell'ambiente.

La presente Parte Speciale, con riferimento ai reati previsti dal D. Lgs. 121/2011 (di seguito anche “Reati ambientali”) illustra i comportamenti che devono essere tenuti dai Soggetti che operano nelle relative aree a rischio reato.

### **7.3. Le fattispecie di reato richiamate dal D.Lgs 231/01**

Il 7 luglio 2011 il Consiglio dei Ministri ha approvato il D. Lgs. 121/2011 recependo la direttiva 2008/99/CE concernente la tutela penale dell'ambiente, nonché la Direttiva 2009/123/CE relativa all'inquinamento provocato dalle navi.

L'attività normativa si sostanzia nell'introduzione dell'Art. 25-undecies del D.Lgs 231/01 con relative sanzioni per violazioni e l'estensione della responsabilità amministrativa degli enti ad alcuni illeciti commessi in violazione delle norme sulla tutela dell'ambiente.

L'azienda è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali.

A tal fine, ha avviato un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, in considerazione dei reati previsti dagli art. 25 -undecies del Decreto Legislativo 231/01, volto a verificare la rispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto.

In considerazione delle caratteristiche societarie ed organizzative, la presente Parte Speciale riguarda i reati previsti dall' art.25-undecies del D.Lgs. 231/01 (di seguito, per brevità, “art. 25 - undecies”), unitamente ai comportamenti che devono essere tenuti dai soggetti ai quali il Modello ex D.Lgs. 231/01 è destinato.

Di seguito, l'elenco dei reati contemplati dall'Art. 25-undecies (di seguito, anche “Reati ambientali”) del Decreto e il testo delle relative disposizioni.

#### **7.3.1. Scarichi di acque reflue (art. 137, D.Lgs 152/2006)**

1. Chiunque apra o comunque effettui nuovi scarichi di acque reflue industriali, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata, è punito con l'arresto da due mesi a due anni o con l'ammenda da millecinquecento euro a diecimila euro.
2. Quando le condotte descritte al comma 1 riguardano gli scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto, la pena è dell'arresto da tre mesi a tre anni.
3. Chiunque, al di fuori delle ipotesi di cui al comma 5, effettui uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni

dell'autorità competente a norma degli articoli 107, comma 1, e 108, comma 4, è punito con l'arresto fino a due anni.

... .. (omissis)

5. Chiunque, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del presente decreto, nell'effettuazione di uno scarico di acque reflue industriali, superi i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del presente decreto, oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1, è punito con l'arresto fino a due anni e con l'ammenda da tremila euro a trentamila euro. Se sono superati anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5, si applica l'arresto da sei mesi a tre anni e l'ammenda da seimila euro a centoventimila euro

... .. (omissis)

11. Chiunque non osservi i divieti di scarico previsti dagli articoli 103 e 104 è punito con l'arresto sino a tre anni

... .. (omissis)

13. Si applica sempre la pena dell'arresto da due mesi a due anni se lo scarico nelle acque del mare da parte di navi od aeromobili contiene sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente

Le singole condotte sanzionate dal comma 1 dell'articolo 137, richiamate dal comma 2 dello stesso articolo 137, rilevano quattro comportamenti illeciti, consistenti:

- nell'apertura ovvero nell'effettuazione di nuovi scarichi di acque reflue industriali senza autorizzazione
- nell'effettuazione ovvero nel mantenimento di scarichi di acque reflue industriali dopo che l'autorizzazione sia stata sospesa o revocata

Le prime due condotte sanzionano, dunque, il comportamento sia di chi attiva fisicamente lo scarico, sia di chi subentra nella gestione di uno scarico aperto da altri, senza, in entrambi i casi, avere la prescritta autorizzazione. Ne discende che la norma in commento è volta a condannare una condizione di abusività degli scarichi, ovvero quegli scarichi privi in origine del titolo abilitativo.

Le rimanenti due condotte sanzionano, invece, una condizione di abusività sopravvenuta, ovvero quei casi in cui l'illiceità dello scarico sopravviene ad un provvedimento amministrativo successivo all'autorizzazione che ne sospende o ne revoca l'efficacia.

La condotta di cui al comma 3 dell'articolo 137, Codice dell'Ambiente, sanziona la condotta consistente nello scarico di acque reflue industriali contenenti sostanze pericolose con violazione delle prescrizioni contenute nell'autorizzazione o di altre prescrizioni imposte dall'autorità competente, ai sensi degli articoli 107, comma 1 e 108, comma 4.

La condotta di cui al comma 5 dell'articolo 137, Codice dell'Ambiente, sanziona la condotta di chiunque effettui scarichi di acque reflue industriali, superando i valori limite fissati dalla tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del D.Lgs. n.152/2006, ovvero i limiti più restrittivi fissati dalle Regioni o dalle Province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5.

La condotta di cui al comma 11 dell'articolo 137, Codice dell'Ambiente, sanziona l'inosservanza del divieto di scarico sul suolo e negli strati superficiali del sottosuolo, nonché di scarico diretto nelle acque sotterranee e nel sottosuolo sanciti, rispettivamente, dagli articoli 103 e 104, Codice dell'Ambiente, fatte salve le tassative eccezioni contenute negli stessi articoli 103 e 104.

La condotta di cui al comma 13 dell'articolo 137, Codice dell'Ambiente, sanziona penalmente lo scarico nelle acque del mare da parte di navi o aeromobili, che contenga sostanze o materiali per i quali vige il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali ratificate dall'Italia (in primis, la Convenzione Marpol 73/78).

### **7.3.2. Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, D.Lgs 152/2006)**

Si applica la pena di cui all'articolo 483 del codice penale a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.

..... (omissis)

Il comma 4, seconda parte, dell'articolo 258, Codice dell'Ambiente, punisce penalmente le due seguenti condotte illecite:

- 1) la predisposizione di un certificato di analisi dei rifiuti contenente false indicazioni sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti stessi;
- 2) l'uso di un certificato contenente indicazioni false durante il trasporto dei rifiuti.

Tali fattispecie di reato rientrano nel novero dei reati propri, in quanto possono essere commesse solo da soggetti aventi una specifica posizione soggettiva. Nell'ipotesi di predisposizione di un certificato di analisi contenente indicazioni false, tale condotta illecita può essere realizzata solo dalle persone abilitate al rilascio di questi certificati; invece, nell'ipotesi di uso di un certificato di analisi contenente indicazioni false durante il trasporto dei rifiuti, tale condotta è riferibile al trasportatore. Con riferimento all'elemento soggettivo, le fattispecie di reato in esame sono punibili esclusivamente a titolo di dolo.

### **7.3.3. Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, D.Lgs 152/2006)**

6. Si applica la pena di cui all'articolo 483 c.p. a colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.
7. ... .. *(omissis)* Si applica la pena di cui all'art. 483 del codice penale in caso di trasporto di rifiuti pericolosi. Tale ultima pena si applica anche a colui che, durante il trasporto fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.
8. Il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI – AREA Movimentazione fraudolentemente alterata è punito con la pena prevista dal combinato disposto degli articoli 477 e 482 del codice penale. La pena è aumentata fino ad un terzo nel caso di rifiuti pericolosi.  
..... *(omissis)*

Il comma 6 dell'articolo 260-bis, Codice dell'Ambiente, sanziona due condotte illecite, ovvero:

- falsificazione, nell'ambito della predisposizione di un certificato di analisi di rifiuti, utilizzato per il sistema di controllo della tracciabilità dei rifiuti, delle indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti. A tale proposito, si precisa che per l'integrazione della fattispecie di reato occorre non solo la predisposizione del certificato analitico dei rifiuti falso, ma anche l'utilizzo dello stesso nell'ambito del sistema di controllo della tracciabilità dei rifiuti.
- Inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti, nell'ambito del sistema di controllo della tracciabilità dei rifiuti. Con riferimento all'elemento soggettivo, entrambe le fattispecie di reato in esame sono/erano punibili esclusivamente a titolo di dolo.

Il secondo periodo del comma 7 dell'articolo 260-bis, Codice dell'Ambiente, sanziona penalmente la condotta del trasportatore che omette/avesse ommesso di accompagnare il trasporto di rifiuti pericolosi (laddove la natura di «rifiuti pericolosi» è elemento caratterizzante rispetto al primo periodo dello stesso comma).

Il terzo periodo del comma 7 dell'articolo 260-bis, Codice dell'Ambiente, sanziona penalmente la condotta di chi, durante il trasporto di rifiuti, fa uso di un certificato di analisi contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.

Con riferimento all'elemento soggettivo, entrambe le fattispecie di reato in esame sono punibili esclusivamente a titolo di dolo.

Il comma 8, dell'articolo 260-bis, Codice dell'Ambiente, sanziona penalmente la condotta illecita del trasportatore che accompagna i rifiuti (non pericolosi, per quanto attiene al primo periodo, e pericolosi per il secondo).

### **7.3.4. Superamento valori limite di emissione (art. 279, D.Lgs 152/2006)**

..... *(omissis)*

2. Chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del presente decreto, dai piani e dai programmi dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorità competente ai sensi del presente titolo è punito con l'arresto fino ad un anno o con l'ammenda fino a 1.032 euro. Se i valori limite le prescrizioni violati sono contenuti nell'autorizzazione integrata ambientale si applicano le sanzioni previste dalla normativa che disciplina tale autorizzazione.

..... (omissis)

5. Nei casi previsti dal comma 2 si applica sempre la pena dell'arresto fino ad un anno se il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

..... (omissis)

Il comma 2 dell'articolo 279, Codice dell'Ambiente, sanziona la condotta di colui che "nell'esercizio di uno stabilimento" violi i valori limite di emissione o le prescrizioni stabiliti:

- dall'autorizzazione
- dagli Allegati I, II, III o V alla parte quinta del Codice dell'Ambiente
- dai piani e dai programmi citati nell'articolo 271, Codice dell'Ambiente
- dalla normativa di cui all'articolo 271 del Codice dell'Ambiente
- dall'autorità competente
- dall'autorizzazione integrata ambientale.

#### **7.3.5. Falsificazione o alterazione di certificati e licenze (art. 3-bis, Legge 150/1992)**

Alle fattispecie previste dall'articolo 16, paragrafo 1, lettere a), c), d), e), ed l), del Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996, e successive modificazioni, in materia di falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni al fine di acquisizione di una licenza o di un certificato, di uso di certificati o licenze falsi o alterati si applicano le pene di cui al libro II, titolo VII, capo III del codice penale.

Ai fini della responsabilità amministrativa degli enti introdotta dall'articolo 25-undecies del Decreto, rilevano i reati del codice penale richiamati dal comma n. 1, in relazione alla falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, ovvero alla comunicazione di informazioni al fine di acquisire una licenza o un certificato, ovvero ancora all'utilizzo di certificati o licenze falsi o alterati. Si tratta, in particolare, dei delitti di cui al Libro Secondo, Titolo VII, Capo III del codice penale (i.e.: Falsità in atti, di cui agli articoli dal 476 al 493-bis, c.p.).

Le condotte sanzionate sono variegata e coprono le diverse ipotesi di falsità (materiale o ideologica) in atti commesse dal privato o dal pubblico ufficiale in relazione ai certificati, licenze o altri documenti rientranti nella disciplina di cui alla Legge n. 150/1992.

#### **7.3.6. Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3-bis, Legge 150/1992)**

1. La produzione, il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione delle sostanze lesive di cui alla tabella A allegata alla presente legge sono regolati dalle disposizioni di cui al regolamento (CE) n. 3093/94.
2. A decorrere dalla data di entrata in vigore della presente legge è vietata l'autorizzazione di impianti che prevedano l'utilizzazione delle sostanze di cui alla tabella A allegata alla presente legge, fatto salvo quanto disposto dal regolamento (CE) n. 3093/94.
3. Con decreto del Ministro dell'ambiente, di concerto con il Ministro dell'industria, del commercio e dell'artigianato, sono stabiliti, in conformità alle disposizioni ed ai tempi del programma di eliminazione progressiva di cui al regolamento (CE) n. 3093/94, la data fino alla quale è consentito l'utilizzo di sostanze di cui alla tabella A, allegata alla presente legge, per la manutenzione e la ricarica di apparecchi e di impianti già venduti ed installati alla data di entrata in vigore della presente legge, ed i tempi e le modalità per la cessazione dell'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, e sono altresì individuati gli usi essenziali delle sostanze di cui alla tabella B, relativamente ai quali possono essere concesse deroghe a quanto previsto dal presente comma. La produzione, l'utilizzazione, la commercializzazione, l'importazione e l'esportazione delle sostanze di cui alle tabelle A e B allegata alla presente legge cessano il 31 dicembre 2008, fatte salve le sostanze, le lavorazioni e le produzioni non comprese nel campo di applicazione del regolamento (CE) n. 3093/94, secondo le definizioni ivi previste.
4. L'adozione di termini diversi da quelli di cui al comma 3, derivati dalla revisione in atto del regolamento (CE) n. 3093/94, comporta la sostituzione dei termini indicati nella presente legge ed il contestuale adeguamento ai nuovi termini.
5. Le imprese che intendono cessare la produzione e l'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, prima dei termini prescritti possono concludere appositi accordi di programma con i Ministeri dell'industria, del commercio e dell'artigianato e dell'ambiente, al fine di usufruire degli incentivi di cui all'articolo

10, con priorità correlata all'anticipo dei tempi di dismissione, secondo le modalità che saranno fissate con decreto del Ministro dell'industria, del commercio e dell'artigianato, d'intesa con il Ministro dell'ambiente.

6. Chiunque viola le disposizioni di cui al presente articolo è punito con l'arresto fino a due anni e con l'ammenda fino al triplo del valore delle sostanze utilizzate per fini produttivi, importate o commercializzate. Nei casi più gravi, alla condanna consegue la revoca dell'autorizzazione o della licenza in base alla quale viene svolta l'attività costituente illecito.

In particolare, i comportamenti disciplinati dall'articolo 3 della Legge n. 549/1993 hanno ad oggetto una serie di condotte che trovano la loro disciplina (ed il regime delle eventuali esenzioni o deroghe applicabili) nel Regolamento (CE) n. 1005/2010, in tema di:

- produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive di cui alla Tabella A alla Legge n. 549/1993;
- autorizzazione di impianti che prevedano l'utilizzazione delle sostanze lesive di cui alla Tabella A alla Legge n. 549/1993;
- utilizzazione delle sostanze di cui alla Tabella A alla Legge n. 549/1993 per la manutenzione di apparecchi ed impianti già venduti ed installati, nonché tempi e modalità per la cessazione dell'utilizzazione delle sostanze di cui alla Tabella B alla Legge n. 549/1993.

#### **7.4. Le attività sensibili relative ai reati ambientali**

Con riferimento alle fattispecie disciplinate dall'art.25-undecies del D.Lgs. 231/01, sono state individuate le principali aree a rischio reato in cui l'azienda potrebbe essere coinvolta e le attività da ritenersi maggiormente "sensibili", ossia quelle attività il cui svolgimento espone la Società al rischio di commissione dei reati individuati nell'ambito della normativa di riferimento.

Di seguito si riportano le "aree a rischio reato" con riferimento alle fattispecie di cui all'art.25-undecies del D.Lgs.231/01 con una breve descrizione delle attività che le compongono.

##### **1. GESTIONE DI RACCOLTA E TRASPORTO RIFIUTI NON – PERICOLOSI**

- Attività di identificazione, caratterizzazione e classificazione dei rifiuti;
- Attività di raccolta e deposito temporaneo dei rifiuti;
- Selezione e gestione dei fornitori per l'attività di trasporto e smaltimento dei rifiuti.

##### **2. GESTIONE DEGLI ADEMPIMENTI E DELLE ATTIVITÀ CONNESSI ALLA NOTIFICA ED ALLA BONIFICA, A SEGUITO DI UN EVENTO CHE SIA POTENZIALMENTE IN GRADO DI CONTAMINARE IL SUOLO, IL SOTTOSUOLO, LE ACQUE SUPERFICIALI E/O LE ACQUE SOTTERRANEE**

- Comunicazione di eventi che siano potenzialmente in grado di contaminare il suolo, il sottosuolo, le acque superficiali e/o le acque sotterranee;
- Attività di bonifica di suolo, sottosuolo, acque superficiali e/o acque sotterranee.

##### **3. GESTIONE DEGLI IMPIANTI PER LA RACCOLTA, IL TRATTAMENTO E LO SMALTIMENTO DELLE ACQUE METEORICHE DI DILAVAMENTO RICADENTI SULLE AREE SOCIETARIE.**

#### **7.5. Organi e funzioni aziendali coinvolte**

In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti gli organi e funzioni aziendali che svolgono attività correlabili a:

- **Servizio Tecnico:** Funzione che si occupa della gestione della manutenzione di beni mobili/immobili e della progettazione e della realizzazione di risorse infrastrutturali logistiche.
- **Direzione:** funzione che si occupa dell'organizzazione e gestione delle iniziative di sponsorizzazione e beneficenza.
- **Ufficio Tecnico:** Come referente per la gestione di interventi di manutenzione ordinaria straordinaria di beni immobili e mobili, la raccolta e la gestione dei rifiuti e la progettazione/realizzazione di infrastrutture logistiche.

## 7.6. Principi e regole di comportamento

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, la politica e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda.

In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli amministratori, gli organi sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- **La normativa italiana e straniera applicabile alle attività svolte;**
- **Il Codice Etico Aziendale;**
- **Le disposizioni contenute nel presente Modello;**
- **Le procedure e le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della Società.**

## 7.7. Principi e norme generali di comportamento

La presente Parte Speciale è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a rischio reato e nello svolgimento delle attività sensibili.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale e al fine di perseguire la prevenzione dei reati ambientali è fatto espresso divieto a tutti i soggetti destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-undecies del D.Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale.

È da considerarsi vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplata dall'art.25-undecies del D.Lgs. 231/01.

In generale, la prevenzione dei reati ambientali è svolta attraverso adeguate misure organizzative e normative e in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- **Previsione nel Codice Etico e relativa appendice applicativa di specifiche indicazioni volte a impedire la commissione dei reati previsti dall'art.25-undecies del D.Lgs. 231/01;**
- **Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino i sistemi di controllo preventivi o le indicazioni comportamentali presenti nel Modello e in tutta la documentazione societaria esistente e ad esso afferente;**
- **Predisposizione di adeguati strumenti organizzativi e normativi atti a prevenire e/o impedire la realizzazione dei reati previsti dall'art. 25 - undecies del D.Lgs. 231/01 da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio;**
- **Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dall'art. 25 - undecies del D.Lgs. 231/01.**

Conseguentemente, gli organi sociali, gli amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento della attività a rischio hanno l'espresso obbligo di perseguire i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

- **Segregazione delle attività**  
Si richiede l'applicazione del principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio, tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso.
- **Esistenza di procedure**  
Devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le

responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività.

– **Poteri autorizzativi e di firma**

Definire livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio. Inoltre i poteri autorizzativi e di firma devono: essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese e essere chiaramente definiti e conosciuti all'interno della società.

– **Tracciabilità**

Tracciabilità delle attività svolte nell'ambito dei processi esposti a rischio; ogni operazione relativa alle attività sensibili deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

– **Gestione delle segnalazioni**

Raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati ambientali rilevati da soggetti interni e esterni all'ente.

– **Riporto all'OdV (Organismo di Vigilanza)**

Riferire prontamente all'OdV eventuali situazioni di irregolarità .

### 7.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), gli organi sociali, gli amministratori, i dipendenti e i aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nelle svolgimento delle attività a rischio sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25 - undecies del D.Lgs. 231/01, al rispetto delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio.

Tra le regole e procedure che prevedono le modalità per lo svolgimento delle attività necessarie a mitigare i fattori di rischio caratteristici delle aree a rischio identificate ed i relativi controlli, si elencano:

- L'esistenza di un sistema di deleghe di funzioni tale da garantire, in capo al soggetto delegato, oltre alle competenze specifiche, la sussistenza di poteri decisionali coerenti con le deleghe assegnate ed un potere di spesa adeguato, per l'efficace adempimento delle funzioni delegate in merito al rispetto della normativa ambientale;
- La redazione di piani in materia di ambiente, approvati dagli organi societari competenti, che individuino i soggetti coinvolti, scadenze e risorse necessarie per l'attuazione (finanziarie, umane, logistiche, di equipaggiamento) e che siano comunicati al personale interessato al fine di garantirne una adeguata comprensione;
- L'esistenza di un processo di gestione dell'affidamento dei compiti specifici ai lavoratori in tema di ambiente;
- L'aggiornamento delle informazioni riguardo alla legislazione rilevante per le tematiche ambientali, ivi inclusi i criteri e le modalità per la comunicazione di tali aggiornamenti alle funzioni aziendali interessate;
- La gestione delle attività di ottenimento, modifica e/o rinnovo delle autorizzazioni ambientali, affinché siano svolte in osservanza alle prescrizioni normative vigenti. In particolare, tale strumento deve prevedere responsabilità e modalità di:
  - a. Identificazione della necessità di richiesta di una nuova autorizzazione o di modifica di autorizzazioni preesistenti
  - b. Monitoraggio delle tempistiche per l'ottenimento del rinnovo delle autorizzazioni esistenti
  - c. Predisposizione dell'idonea documentazione prevista dall'iter autorizzativo (ad esempio la predisposizione di studi di impatto ambientale, le valutazioni di incidenza nell'ambito dei progetti presentati, etc.)
  - d. Comunicazione dell'avvenuto ottenimento dell'autorizzazione, sua modifica e/o rinnovo alle figure interessate
  - e. Tracciabilità dell'iter autorizzativo dalla raccolta dei dati fino alla comunicazione dell'esito dello stesso
- La gestione delle emergenze ambientali, ivi inclusi il recepimento dei miglioramenti tecnologici del settore e le modalità e la tempistica/frequenza di svolgimento delle prove di emergenza;
- La gestione della manutenzione degli asset e dei sistemi di prevenzione, protezione e mitigazione ambientali, affinché sia sempre garantita l'integrità e l'adeguatezza in termini di tutela dell'ambiente;

- L'identificazione e valutazione dei rischi ambientali, nonché l'identificazione degli aspetti ambientali e valutazione della loro significatività in funzione degli impatti ambientali diretti e indiretti ad essi correlati, per servizi resi e attività svolte in condizioni operative normali, anomale, in condizioni di avviamento e di fermata e in situazioni di emergenza e di incidenti;
- La gestione dell'attività finalizzate alla bonifica dei siti contaminati, che preveda, a seguito di un evento che sia potenzialmente in grado di contaminare il suolo, il sottosuolo, le acque superficiali e/o le acque sotterranee:
  - a. L'identificazione di elementi che facciano presumere una potenziale contaminazione (attuale o storica), ai fini della valutazione dell'avviamento delle necessarie attività di comunicazione e/o bonifica;
  - b. La comunicazione da effettuarsi alle autorità competenti, al verificarsi di un evento che sia potenzialmente in grado di contaminare, ovvero all'atto di contaminazione del suolo, del sottosuolo, delle acque superficiali e/o delle acque sotterranee, in linea con le modalità e tempistiche previste dalla normativa vigente;
  - c. La definizione e il monitoraggio delle procedure operative ed amministrative per la predisposizione della documentazione da presentare alle autorità competenti, nel rispetto delle modalità e delle tempistiche previste dalla normativa vigente;
  - d. La verifica della realizzazione degli interventi di bonifica in linea con quanto previsto dal progetto di bonifica approvato;
  - e. La predisposizione della documentazione da presentare alle Autorità competenti al completamento dell'intervento, ai fini del rilascio della certificazione di avvenuta bonifica.
- Rifiuti pericolosi aventi differenti caratteristiche di pericolosità, ovvero dei rifiuti pericolosi con rifiuti non pericolosi, sostanze e/o altri materiali;
- La gestione dei depositi temporanei di rifiuti, prevedendo:
  - a. La definizione dei criteri per la scelta / realizzazione delle aree adibite al deposito temporaneo di rifiuti o l'identificazione delle aree destinate al deposito temporaneo di rifiuti;
  - b. La raccolta dei rifiuti per categorie omogenee e l'identificazione delle tipologie di rifiuti ammessi all'area adibita a deposito temporaneo.
- La gestione della documentazione relativa al sistema di controllo per le tematiche ambientali (ivi compresa l'archiviazione e la conservazione);
- La gestione delle attività di audit e verifica periodica dell'efficienza ed efficacia del sistema di controllo per le tematiche ambientali, con riferimento a:
  - a. Tempistica per la programmazione delle attività (piano di audit formalizzato);
  - b. Competenze necessarie per il personale coinvolto nelle attività di audit nel rispetto del principio dell'indipendenza dell'auditor rispetto all'attività oggetto di audit;
  - c. Modalità di individuazione e applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di controllo relativo alle tematiche ambientali o dalle norme e prescrizioni applicabili;
  - d. Modalità di verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;
  - e. Modalità di comunicazione dei risultati dell'audit al responsabile del rispetto della normativa ambientale.
- La gestione delle attività di reporting verso il responsabile del rispetto della normativa ambientale, tali da garantire la tracciabilità e la disponibilità dei dati relativi alle attività inerenti al sistema di controllo e in particolare l'invio periodico delle informazioni inerenti a:
  - a. Scostamenti tra i risultati ottenuti e gli obiettivi programmati;
  - b. Risultati degli audit;
  - c. Risultati del monitoraggio della performance del sistema di controllo ambientale.
- Verifica della situazione nella gestione delle tematiche ambientali e di una adeguata diffusione delle risultanze delle riunioni all'interno della società;
- La gestione della diffusione periodica verso i lavoratori, da parte delle funzioni competenti, delle informazioni connesse alla normativa vigente relativa all'ambiente;
- La gestione del processo di formazione del personale in materia ambientale.

### **7.9. Impegni per la salvaguardia ambientale**

L'azienda è consapevole che l'impegno costante verso la compatibilità ambientale, al fine di prevenire, nel rispetto della legislazione, l'inquinamento, e una gestione razionale delle risorse naturali rappresentino un'opportunità di

sviluppo per l'azienda, migliorandone l'immagine nel contesto sociale in cui opera e contribuendo alla soddisfazione dei clienti finali.

La società persegue l'obiettivo di coniugare le esigenze lavorative con la salvaguardia ambientale, definendo un piano per il miglioramento continuo della gestione ambientale, che tenga conto delle seguenti linee guida:

- **Costante ricerca delle soluzioni tecnologiche più promettenti in materia di tutela ambientale;**
- **Assegnazione di responsabilità gestionali per l'ambiente nelle attività aziendali;**
- **Coinvolgimento dei dipendenti e dei fornitori sulle tematiche ambientali con azioni orientate al miglioramento continuo;**
- **Implementazione dei Sistemi di Gestione Ambientale, certificati secondo standard internazionali;**
- **Adozione di un sistema di monitoraggio delle performance ambientali.**

#### **7.10. Controlli dell'Organismo di Vigilanza**

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale.

Tali controlli sono diretti a verificare la corretta applicazione dei principi e delle regole generali di comportamento del presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

Inoltre, i compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui alla presente Parte Speciale:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati ambientali;
- monitorare sul rispetto delle procedure interne per la prevenzione dei suddetti reati;
- monitoraggio specifico sulle attività sensibili dell'azienda che la espongono ai reati esaminati nella presente Parte Speciale;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente dell'azienda ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.