

LUMAGEST S.R.L.

a socio unico

**Modello di Organizzazione, Gestione e Controllo ex Decreto Legislativo 8 giugno
2001, n. 231**

15 settembre 2023

DEFINIZIONI.....	7
PARTE GENERALE.....	9
1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento	10
1.2 Presupposti di esclusione della responsabilità dell'ente.....	12
1.3 La Società	14
1.4 L'adozione del Modello.....	15
1.5 Funzione e scopo del Modello	16
1.6 La costruzione del Modello e la sua struttura	16
1.7 Modifiche e integrazioni del Modello	18
1.8 Destinatari del Modello	18
CAPITOLO 2	19
2.1 Il sistema in linea generale	19
CAPITOLO 3	20
3.1 Identificazione dell'Organismo di Vigilanza	20
3.2 Funzione, poteri e compiti dell'Organismo di Vigilanza.....	23
3.3 Reporting dell'OdV nei confronti degli Organi Sociali	25
3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza.....	26
3.5 <i>Whistleblowing</i>	27
3.6 Obblighi di riservatezza.....	29
3.7 Raccolta e conservazione delle informazioni	29
CAPITOLO 4	30
4.1 Formazione ed informazione dei Dipendenti.....	30
4.2 Selezione e Informazione dei Consulenti, degli <i>Outsourcer</i> , dei Fornitori e delle controparti contrattuali della Società	31
CAPITOLO 5	32
5.1 Funzione del sistema sanzionatorio	32
5.2 Sistema sanzionatorio dei Dipendenti.....	32
5.3 Misure nei confronti degli Amministratori.....	34
5.4 Misure nei confronti dei Sindaci (ove nominati)	34
5.5 Misure nei confronti dei Consulenti, degli <i>Outsourcer</i> , dei Fornitori e delle controparti contrattuali della Società	34
PARTI SPECIALI.....	36

PARTE SPECIALE – A – REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE	37
LE FATTISPECIE DI REATO	38
Le fattispecie dei reati nei rapporti con la P.A. (artt. 24 e 25, D.Lgs. 231/2001).....	38
CRITERI PER LA DEFINIZIONE DI P.A. E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO	44
A.2.1 Enti della pubblica amministrazione.....	44
A.2.2 Pubblici Ufficiali.....	45
A.2.3 Incaricati di un pubblico servizio.....	46
A.3.1 Attività Sensibili in relazione ai reati nei rapporti con la P.A. e al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.....	48
A.3.2 Attività Strumentali alla commissione di reati nei rapporti con la P.A. e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci.....	48
A.4.1 Il sistema in linea generale	49
A.4.2 Il sistema di deleghe e procure	49
A.4.3 Principi generali di comportamento.....	50
Principi specifici di comportamento.....	52
CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	56
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	57
PARTE SPECIALE – B – REATI SOCIETARI	59
LE FATTISPECIE DI REATO.....	60
Le fattispecie dei reati societari (art. 25 <i>ter</i>, D.Lgs. n. 231/2001)	60
B.2.1 Attività Sensibili nell'ambito dei Reati Societari	67
REGOLE GENERALI.....	68
B.3.1 Il sistema in linea generale	68
B.3.2 Principi generali di comportamento.....	68
Principi specifici di comportamento.....	70
CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	72
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	73
CAPITOLO C.1.....	75
Le fattispecie di reato	75
CAPITOLO C.2.....	81

C.2.1 Attività Sensibili nell'ambito dei Reati di Ricettazione, Riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché Autoriciclaggio e dei Reati con finalità di Terrorismo e Delitti in materia di strumenti di pagamento diversi dai contanti	81
CAPITOLO C.4	83
Principi comportamentali specifici	83
CAPITOLO C.5.....	86
CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	86
CAPITOLO C.6.....	87
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	87
PARTE SPECIALE – D – REATI DI OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO	88
REATI CONTRO LA PERSONALITÀ INDIVIDUALE E IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE	88
DEFINIZIONI:.....	89
CAPITOLO D.1	91
LE FATTISPECIE DI REATO	91
Le fattispecie di Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello stato e favoreggiamento dell'immigrazione clandestina (art. 25- <i>duodecies</i> D.Lgs. 231/2001).....	92
CAPITOLO D.3	96
REGOLE GENERALI.....	96
D.3.1 Principi generali di comportamento.....	96
D.3.5 L'attività di monitoraggio	108
CAPITOLO D.4.....	110
I CONTRATTI DI APPALTO E LE ASSUNZIONI DI CITTADINI EXTRA UE	110
CAPITOLO D.5	114
CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	114
CAPITOLO D. 6	115
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	115
PARTE SPECIALE – E – REATI AMBIENTALI	116
CAPITOLO E. 1	117
LE FATTISPECIE DI REATO.....	117
CAPITOLO E.3.....	120
E.3.1 Principi di comportamento	120
CAPITOLO E.4	122

CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	122
CAPITOLO E.5	123
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	123
PARTE SPECIALE – F – REATI DI CRIMINALITÀ ORGANIZZATA	124
CAPITOLO F.1.....	125
Le fattispecie dei reati di criminalità organizzata.....	125
CAPITOLO F.2.....	127
Attività Sensibili	127
CAPITOLO F.3.....	128
REGOLE DI COMPORTAMENTO.....	128
F.3.1 Principi generali di comportamento.....	128
F.3.2 Principi specifici di comportamento	128
CAPITOLO F.4.....	128
CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	128
CAPITOLO F.5.....	130
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	130
PARTE SPECIALE – G – REATI INFORMATICI.....	131
DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE.....	131
CAPITOLO G.1	132
LE FATTISPECIE DI REATO.....	132
Le fattispecie dei reati informatici e dei delitti in violazione del diritto d'autore.....	132
CAPITOLO G.3.....	144
G.3.1 Regole e principi generali.....	144
CAPITOLO G. 5.....	149
CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	149
CAPITOLO G.6	150
FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA	150
PARTE SPECIALE – H – REATI TRIBUTARI.....	151
CAPITOLO H. 1.....	152
H.1.1. Le fattispecie dei reati tributari (art. 25-<i>quinquiesdecies</i>, D. Lgs. n. 231/2001)	152
CAPITOLO H.2.....	156
Attività Sensibili nell'ambito dei reati tributari.....	156
CAPITLO H.3	157
Principi generali di comportamento	157
CAPITOLO H.4.....	158

Principi procedurali specifici	158
CAPITOLO H.5	161
I controlli dell’OdV	161
I.1.1. Le fattispecie dei Delitti contro il patrimonio culturale e reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (artt. 25-<i>septiesdecies</i> e 25-<i>duodevicies</i>, D. Lgs. n. 231/2001)	164
Attività Sensibili nell’ambito dei Delitti contro il patrimonio culturale e reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici	167
Principi generali di comportamento	168
CAPITOLO I.4	169
Principi procedurali specifici	169
A completamento dei presidi previsti nella presente Parte Speciale, con riferimento alla gestione dei rapporti con le Autorità competenti (i.e. la Soprintendenza), si fa rinvio, altresì, ai presidi previsti nella Parte Speciale A per la gestione dei rapporti con la Pubblica Amministrazione.....	170

DEFINIZIONI

Le seguenti definizioni si riferiscono a tutte le parti del Modello di organizzazione, gestione e controllo, fatte salve ulteriori eventuali definizioni contenute nelle singole Parti Speciali.

- **Attività Sensibili:** le attività di Lumagest S.r.l. a socio unico nel cui ambito sussiste il rischio astratto di commissione dei Reati.
- **Attività Strumentali:** quelle attività che, pur non essendo direttamente finalizzate alla commissione del reato, costituiscono comunque attività strumentali alla realizzazione del medesimo (ad esempio, le attività che consentono l'approvvigionamento di risorse finanziarie necessarie al soggetto corruttore, nonché quelle che costituiscono di per sé merce di scambio da offrire al soggetto corrotto, la selezione di Consulenti compiacenti e destinati a porre in essere Reati nell'interesse della Società, ecc.).
- **Organo amministrativo:** il Consiglio di Amministrazione o l'Amministratore Unico di Lumagest S.r.l. a socio unico
- **CCNL:** il Contratto Collettivo Nazionale di Lavoro (*i.e.* Contratto Collettivo Nazionale di Lavoro per i dipendenti delle industrie metalmeccaniche private e della installazione di impianti) attualmente in vigore e applicato dalla Società.
- **Consulenti:** i soggetti che agiscono in nome e/o per conto della Società in forza di un contratto di consulenza, di un mandato o di altro rapporto contrattuale di collaborazione.
- **Destinatari:** gli Organi Sociali, gli *Outsourcer*, i Consulenti, i Fornitori e in genere le controparti contrattuali della Società.
- **Dipendenti:** i soggetti che hanno (o avranno in futuro) un rapporto di lavoro subordinato con Lumagest S.r.l. a socio unico o coloro che svolgeranno attività lavorativa per la Società in forza di un contratto con la stessa (ivi compresi i dirigenti e gli stagisti).
- **D. Lgs. n. 231/2001 o Decreto o Decreto 231:** il Decreto Legislativo 8 giugno 2001, n. 231 e sue successive modificazioni e integrazioni.
- **Fornitori:** tutti i fornitori di beni e servizi della Società.
- **Linee Guida:** le Linee Guida per la costruzione del modello di organizzazione, gestione e controllo *ex* D.Lgs. 231/2001 emanate dalle principali associazioni a livello nazionale (ad esempio, da Confindustria).

- **Lumagest S.r.l. a socio unico (di seguito “Lumagest” o la “Società”):** Lumagest S.r.l. a socio unico, Via Giuseppe Zampieri, 15, Vicenza.
- **Modello o Modello 231:** il modello di organizzazione, gestione e controllo previsto dal D.Lgs. n. 231/2001.
- **Organo Dirigente:** l’Organo Amministrativo.
- **Organi Sociali:** Organo Amministrativo, Collegio Sindacale (ove nominato), Assemblea dei Soci.
- **Organismo di Vigilanza o OdV:** organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull’osservanza del Modello nonché all’opportunità di un suo aggiornamento, previsto dall’art. 6, comma I, lett. *b*), D.Lgs. 231/2001.
- **Outsourcer:** società terze che prestano in favore di Lumagest S.r.l. attività di erogazione di servizi.
- **Reati o Reati presupposto:** le fattispecie di reati ai quali si applica la disciplina prevista dal D.Lgs. 231/2001, anche a seguito di sue successive modificazioni ed integrazioni.

PARTE GENERALE

IL DECRETO LEGISLATIVO N. 231/2001

1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all’art. 11 della legge 29 settembre 2000 n. 300 – il D.Lgs. 231/2001, entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l’Italia ha già da tempo aderito.

Il D.Lgs. 231/2001, recante la “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*” ha introdotto per la prima volta in Italia la responsabilità in sede penale degli enti per alcuni reati commessi nell’interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

La nuova responsabilità introdotta dal Decreto 231 mira a coinvolgere nella punizione di taluni illeciti di rilevanza penale il patrimonio degli enti che abbiano tratto un interesse o un vantaggio dalla commissione dell’illecito. Per tutti gli illeciti commessi è sempre prevista l’applicazione di una sanzione pecuniaria; per i casi più gravi sono previste anche misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione, l’interdizione dall’esercizio dell’attività, l’esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

La responsabilità prevista dal Decreto 231 si configura anche in relazione ai reati commessi all’estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato medesimo.

Quanto alla **tipologia dei reati c.d. presupposto**, ad oggi gli stessi risultano essere i seguenti:

- (i) *i reati commessi nei rapporti con la Pubblica Amministrazione* (artt. 24 e 25 come modificati dalla Legge 6 novembre 2012, n. 190 e successivamente dalla Legge 9 gennaio 2019, n. 3);
- (ii) *i reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento* (art. 25 bis introdotto dal D.L. 25 settembre 2001, n. 350,

modificato dalla Legge 23 luglio 2009, n. 99 e successivamente dal D. Lgs. 125/2016);

- (iii) i *reati societari* (art. 25 ter introdotto dal D. Lgs. 11 aprile 2002, n. 61, successivamente integrato con il reato di “*corruzione tra privati*” dalla Legge 6 novembre 2012, n. 190 e poi modificato dal D. Lgs. 15 marzo 2017, n. 38 con l’introduzione, inoltre, del reato di “*istigazione alla corruzione tra privati*”, entrambi successivamente modificati dalla Legge 9 gennaio 2019, n. 3);
- (iv) i *reati con finalità di terrorismo o di eversione dell’ordine democratico* (art. 25 quater introdotto dalla Legge 14 gennaio 2003, n. 7);
- (v) pratiche di *mutilazione degli organi genitali femminili* (art. 25 quater.1 introdotto dalla Legge 9 gennaio 2006, n. 7);
- (vi) i *reati contro la personalità individuale* (art. 25 quinquies introdotto dalla Legge 11 agosto 2003, n. 228); la Legge 29 ottobre 2016, n. 199 ha introdotto alcune fattispecie – che rilevano nell’ambito della categoria dei reati contro la personalità individuale – relative al fenomeno del lavoro nero e allo sfruttamento del lavoro in agricoltura (c.d. *caporalato*);
- (vii) i *reati e gli illeciti amministrativi di abuso di mercato* (art. 25 sexies introdotto dalla Legge 18 aprile 2005, n. 62);
- (viii) i *reati transnazionali* (introdotti dalla Legge 16 marzo 2006, n. 146);
- (ix) i *reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro* (art. 25 septies introdotto dalla Legge 3 agosto 2007, n. 123 e successivamente sostituito dal D. Lgs. 9 aprile 2008, n. 81);
- (x) i *reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio* (art. 25 octies introdotto dal D. Lgs. 21 novembre 2007, n. 231 e modificato dalla l. 186/2014);
- (xi) i *delitti in materia di strumenti di pagamento diversi dai contanti* (art. 25-octies.1 introdotto dal Decreto Legislativo 8 novembre 2021, n. 184);
- (xii) i *delitti informatici e il trattamento illecito dei dati* (art. 24 bis introdotto dalla Legge 18 marzo 2008, n. 48);
- (xiii) *delitti contro l’industria e il commercio* (art. 25 bis.1 introdotto dalla Legge 23 luglio 2009, n. 99);

- (xiv) *delitti in materia di violazione del diritto d'autore* (art. 25 novies introdotto dalla Legge 23 luglio 2009, n. 99);
- (xv) *i reati di criminalità organizzata* (art. 24 ter introdotto dalla Legge 15 luglio 2009, n. 94);
- (xvi) *il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria* (art. 25 decies introdotto dalla Legge 3 agosto 2009, n. 116);
- (xvii) *reati ambientali* (art. 25 undecies introdotto dal D. Lgs. 7 luglio 2011, n. 121 e successivamente integrato dalla l. 22 maggio 2015, n. 68);
- (xviii) *impiego di cittadini di paesi terzi il cui permesso di soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina* (art. 25 duodecies introdotto dal D. Lgs. 16 luglio 2012, n. 109 e successivamente integrato dalla Legge 17 ottobre 2017, n. 161);
- (xix) *razzismo e xenofobia* (art. 25 terdecies introdotto dalla Legge 20 novembre 2017, n. 167);
- (xx) *frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati* (art. 25 quaterdecies, introdotto dalla Legge 3 maggio 2019, n. 39);
- (xxi) *reati tributari* (art. 25 quinquiesdecies, introdotto dalla Legge 19 dicembre 2019, n. 157 e successivamente integrato con D.Lgs. 14 luglio 2020, n. 75);
- (xxii) *reati di contrabbando* (art. 25 sexiesdecies, introdotto dal Decreto Legislativo 14 luglio 2020, n. 75);
- (xxiii) *reati contro il patrimonio culturale* (art. 25-septiesdecies, introdotto dalla Legge 9 marzo 2022, n. 22);
- (xxiv) *riciclaggio di beni culturali e devastazione e saccheggio di beni culturali paesaggistici* (art. 25-duodevicies, introdotto dalla Legge 9 marzo 2022, n. 22).

Altre fattispecie di reato potranno in futuro essere inserite dal legislatore nella disciplina dettata dal D.Lgs. 231/2001.

1.2 Presupposti di esclusione della responsabilità dell'ente

Il D.Lgs. n. 231/2001 prevede, agli artt. 6 e 7, una forma di esonero dalla responsabilità qualora la società dimostri di aver adottato ed efficacemente attuato un **modello di**

organizzazione, gestione e controllo idoneo a prevenire la realizzazione dei Reati presupposto. Il Modello deve rispondere alle seguenti esigenze:

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

Il D.Lgs. n. 231/2001 prevede altresì, al fine di permettere la sussistenza dell'esimente in parola, che:

1. la società abbia provveduto all'istituzione di un **organo di controllo** interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello nonché di curarne l'aggiornamento;
2. l'organo di controllo non sia colpevole di omessa o insufficiente vigilanza in merito all'attuazione e all'osservanza del Modello;
3. la società abbia predisposto un sistema di verifica periodica e di eventuale aggiornamento del Modello;
4. l'autore del reato abbia agito eludendo fraudolentemente le disposizioni del Modello.

Lo stesso Decreto dispone che il Modello può essere adottato, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (ovverosia le "Linee Guida") redatti da associazioni rappresentative di categoria.

LE LINEE GUIDA DELLE ASSOCIAZIONI DI CATEGORIA

Nella predisposizione del presente Modello, Lumagest si è ispirata alle Linee Guida elaborate dalle principali associazioni a livello nazionale. I punti fondamentali individuati dalle citate Linee Guida possono essere così sintetizzati:

- individuazione e analisi delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;

- predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di apposite procedure e principi di comportamento. Le componenti più rilevanti del sistema di controllo sono individuate nei seguenti strumenti:
 - codice etico (o di condotta);
 - sistema organizzativo;
 - procedure aziendali;
 - poteri autorizzativi e di firma;
 - sistemi di controllo e gestione;
 - comunicazione e formazione.

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

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
 - i. autonomia e indipendenza;
 - ii. professionalità;
 - iii. continuità di azione.
- obblighi di informazione dell'Organismo di Vigilanza.

IL MODELLO DI LUMAGEST

1.3 La Società

Lumagest è una società che opera nell'ambito della pubblica illuminazione, dell'efficientamento energetico, delle attività di riqualificazione energetica e legate alla mobilità sostenibile.

La Società ha per oggetto, tra le altre, le seguenti principali attività: *“il concorso ad appalti sia pubblici che privati relativi alla gestione integrata del servizio di pubblica illuminazione e connessi interventi di efficientamento energetico, direttamente o in raggruppamento temporaneo con altri soggetti o nell'ambito di costituendo/i consorzio/i stabile/i e comunque in tutte le modalità previste dalla legislazione in merito di*

appalti pubblici e dal codice civile; la progettazione, realizzazione, manutenzione e gestione delle opere di cui alle gare aggiudicate; la gestione dei servizi di cui alle gare aggiudicate [...]; la progettazione, la realizzazione, la manutenzione e la gestione ordinaria e straordinaria degli impianti di illuminazione pubblica, votiva, industriale e d'interni di Comuni, Province, soggetti titolari di concessioni autostradali [...]; la prestazione di servizi legati al miglioramento delle prestazioni energetiche nel settore pubblico e privato, quali: 1) la progettazione, lo sviluppo, la realizzazione, la manutenzione e la gestione ordinaria e straordinaria di servizi smart city; 2) la progettazione, lo sviluppo, la realizzazione, la manutenzione e la gestione ordinaria e straordinaria di servizi legati al settore della mobilità elettrica e sostenibile, tra i quali il servizio di gestione dei mezzi di trasporto elettrici in modalità "sharing", delle infrastrutture per la ricarica dei mezzi di trasporto elettrici e di spazi pubblici per la costruzione di nuove colonnine di ricarica; 3) la costruzione, la manutenzione o la ristrutturazione degli interventi necessari per la produzione di energia elettrica, completi di ogni connessa opera muraria, nonché di tutti gli impianti elettromeccanici, elettrici, telefonici ed elettronici; 4) la posa in opera, la manutenzione o ristrutturazione nonché la esecuzione della segnaletica stradale non luminosa, verticale, orizzontale e complementare; 5) lo sviluppo e la gestione di comunità energetiche, anche tramite l'installazione di impianti ad energia rinnovabile; 6) l'attività di nolo a caldo e a freddo di macchine e macchinari?.

Lumagest ha un unico socio: City Green Light S.r.l. a sua volta posseduto da investitori istituzionali particolarmente attenti agli aspetti di *governance & compliance* e al rispetto delle norme di trasparenza e di correttezza nello svolgimento degli affari della Società.

1.4 L'adozione del Modello

La Società, al fine di assicurare condizioni di correttezza e di trasparenza nella conduzione della propria attività, a tutela della propria responsabilità, della propria immagine e dei propri azionisti, ha ritenuto opportuno procedere all'adozione del presente Modello e di aggiornarlo costantemente nel tempo tenendo conto della normativa vigente, della giurisprudenza, delle *best practice* aziendali e delle Linee Guida.

A tal fine, la Società ha svolto un'attività di analisi dei rischi con il supporto di consulenti legali specializzati e ha adottato il presente Modello, approvato dall'Organo Amministrativo in data 15 settembre 2023. La Società, in pari data, ha nominato, inoltre, un Organismo di Vigilanza monocratico in possesso dei requisiti descritti al successivo paragrafo 5.1, con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

Tutte le Attività Sensibili devono pertanto essere svolte conformandosi alle leggi vigenti, alle procedure aziendali e alle regole contenute nel presente Modello o a cui il presente Modello fa rinvio o riferimento.

1.5 Funzione e scopo del Modello

Scopo del presente Modello è la costruzione di un sistema strutturato e organico di procedure e flussi informativi, nonché di attività di controllo, da svolgersi anche in via preventiva, volto a prevenire il più possibile la commissione delle diverse tipologie di Reato contemplate dal Decreto 231.

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già operanti, in quanto idonei a valere anche come misure di prevenzione dei Reati e di controllo sui processi coinvolti nelle Attività Sensibili.

Il presente Modello si propone le seguenti finalità:

- sensibilizzare tutti i Destinatari e diffondere a tutti i livelli le regole comportamentali in esso previste e le procedure correlate;
- determinare, in tutti coloro che operano in nome e per conto della Società nell'ambito delle Attività Sensibili, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni *ivi* riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti della Società stessa;
- ribadire che tali forme di comportamento illecito sono fortemente condannate dalla Società in quanto (anche nel caso in cui la stessa fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la Società intende attenersi nell'espletamento della propria attività;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle Attività Sensibili, di intervenire tempestivamente per prevenire o contrastare la commissione dei Reati stessi.

1.6 La costruzione del Modello e la sua struttura

Il presente Modello è così composto:

i. una “Parte Generale”, contenente la descrizione dei Reati, le modalità di costruzione del Modello, le regole relative al funzionamento dell’Organismo di Vigilanza, la diffusione dei contenuti del Modello e il sistema sanzionatorio;

ii.n. 11 “Parti Speciali” predisposte per la prevenzione di alcune categorie di Reato, dalla cui analisi dei rischi effettuata la Società è risultata astrattamente esposta in relazione all’attività svolta dalla stessa, e precisamente:

- Parte Speciale A – Reati commessi nei rapporti con la Pubblica Amministrazione e Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria
- Parte Speciale B – Reati Societari
- Parte Speciale C – Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, reati con finalità di terrorismo e autoriciclaggio e delitti in materia di strumenti di pagamento diversi dai contanti
- Parte Speciale D – Reati di Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, delitti contro la personalità individuale e impiego di cittadini terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell’immigrazione clandestina
- Parte Speciale E – Reati ambientali
- Parte Speciale F – Reati di criminalità organizzata
- Parte Speciale G – Reati informatici e Delitti in violazione del diritto d’autore
- Parte Speciale H – Reati tributari
- Parte Speciale I - Delitti contro il patrimonio culturale e reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici

Si rinvia alle singole Parti Speciali per la descrizione dettagliata delle Attività Sensibili e delle relative fattispecie di Reato.

In particolare, ciascuna delle anzidette Parti Speciali ha la funzione di:

- a) identificare i principi comportamentali specifici che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello ed in particolare della limitazione del rischio di commissione della specifica tipologia di Reati da ognuna di esse considerato;

- b) fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che con lo stesso cooperano, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica previste.

1.7 Modifiche e integrazioni del Modello

Le modifiche e integrazioni del Modello sono rimesse alla competenza dell'Organo Dirigente della Società anche su proposta dell'Organismo di Vigilanza.

Le proposte di modifica e integrazione del Modello potranno essere presentate dall'OdV anche sulla base delle indicazioni provenienti dai responsabili delle aree aziendali o dai Consulenti.

1.8 Destinatari del Modello

Le regole contenute nel presente Modello si rivolgono ai seguenti soggetti:

- a. persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società;
- b. persone che esercitano, anche di fatto, la gestione e il controllo della Società stessa;
- c. tutti i soggetti sottoposti alla direzione o alla vigilanza dei soggetti di cui sopra, inclusi gli stagisti;
- d. limitatamente a quanto specificamente indicato nei relativi accordi contrattuali, ai Consulenti, *Outsourcer*, Fornitori, procuratori e, in genere, a tutti coloro che operano in nome o per conto o comunque nell'interesse della Società e alle controparti contrattuali.

I contenuti del Modello sono comunicati ai Destinatari con modalità idonee ad assicurarne l'effettiva conoscenza, secondo quanto indicato al successivo Capitolo 6 della presente Parte Generale. I Destinatari sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di correttezza e diligenza derivanti dal rapporto giuridico da essi instaurato con la Società.

CAPITOLO 2

REGOLE GENERALI DI COMPORTAMENTO

2.1 Il sistema in linea generale

Nell'espletamento delle Attività Sensibili i Destinatari devono rispettare le regole di comportamento previste dal presente Modello e, nello specifico, quelle indicate nelle singole Parti Speciali.

Oltre al presente Modello, i Destinatari – ciascuno nella misura al medesimo applicabile commisurata all'attività svolta – devono in primo luogo conoscere e rispettare:

1. lo Statuto sociale;
2. il Codice Etico;
3. l'organigramma aziendale;
4. ogni altra normativa interna relativa al sistema di *Corporate Governance*, al sistema di controllo interno e di *reporting* adottato dalla Società (ad esempio, *policy* aziendali, procedure, flussi informativi, ecc.).

Le regole, le *policy* e i principi di cui agli strumenti sopra elencati fanno parte del più ampio sistema di organizzazione e controllo che il Modello intende integrare e che tutti i Destinatari, in relazione al tipo di rapporto in essere con la Società, sono tenuti a conoscere e rispettare.

CAPITOLO 3

L' ORGANISMO DI VIGILANZA

3.1 Identificazione dell'Organismo di Vigilanza

Ai sensi dell'art. 6, lett. b) del Decreto 231, condizione indispensabile per la concessione dell'esimente dalla responsabilità amministrativa è l'attribuzione ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo del compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

In ottemperanza a quanto stabilito dal Decreto 231, la Società ha deciso di attribuire tale compito ad un organismo monocratico composto da un membro esterno avente competenze in ambito legale e in materia di controlli. Tale composizione garantisce il miglior contributo al perseguimento degli obiettivi propri dell'Organismo di Vigilanza, nonché la sussistenza e l'effettività dei requisiti di autonomia, indipendenza e continuità richiesti dalla legge e dalla giurisprudenza prevalente.

Le regole circa il funzionamento, la nomina e la durata dell'OdV sono contenute nel Regolamento adottato dall'OdV stesso.

L'OdV possiede i requisiti di autonomia, indipendenza e professionalità, oltre che di onorabilità e assenza di conflitti di interesse, che si richiedono per tale organismo.

Il componente dell'Organismo di Vigilanza ha un profilo professionale e personale che garantisce l'imparzialità di giudizio, l'autorevolezza e l'eticità della sua condotta.

La Società, pertanto, nella scelta del componente dell'Organismo di Vigilanza ha valutato i seguenti elementi:

a. Autonomia e indipendenza

Il requisito di autonomia e indipendenza presuppone che l'OdV risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (*i.e.* l'Organo Amministrativo).

In sede di nomina dell'OdV, la sua autonomia è assicurata tra l'altro dall'obbligo, in capo all'Organo Amministrativo, di approvare una dotazione annua adeguata di risorse finanziarie, proporzionata alle dimensioni della società e dei controlli da eseguire con risorse esterne, su proposta dell'Organismo di Vigilanza stesso, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri doveri (ad esempio, consulenze specialistiche, ecc.).

L'indipendenza, infine, presuppone che l'Organismo di Vigilanza non si trovi in una

posizione, neppure potenziale, di conflitto d'interessi con la Società, né sia titolare all'interno della stessa di funzioni di tipo operativo che ne minerebbero l'obiettività di giudizio nel momento delle verifiche sul rispetto del Modello.

b. Onorabilità e cause di ineleggibilità

Non possono essere eletti membri dell'Organismo di Vigilanza e, se lo sono, decadono necessariamente ed automaticamente dalla carica:

- i. coloro che si trovano nelle condizioni previste dall'articolo 2382 codice civile, ovvero sia gli inabilitati, interdetti, falliti o condannati ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;
- ii. coloro che siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi del D.Lgs. 6 settembre 2011, n. 159 *“Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia”*;
- iii. coloro che sono stati condannati a seguito di sentenza ancorché non ancora definitiva o emessa *ex artt.* 444 codice procedura penale o, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
 1. per uno dei delitti previsti nel titolo XI del libro V del codice civile (Disposizioni penali in materia di società e consorzi) e nel Regio Decreto 16 marzo 1942, n. 267, e sue successive modifiche od integrazioni (disciplina del fallimento, del concordato preventivo e della liquidazione coatta amministrativa);
 2. a pena detentiva, non inferiore ad un anno, per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento (tra questi si segnalano, a titolo esemplificativo e non esaustivo, i reati di abusivismo bancario e finanziario di cui agli artt. 130 e seguenti del Testo Unico Bancario, i reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate di cui all'art. 453 codice penale, i reati di fraudolento danneggiamento dei beni assicurati e mutilazione fraudolenta della propria persona di cui all'art. 642 codice penale);
 3. per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;

4. alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;
 5. in ogni caso e a prescindere dall'entità della pena per uno o più illeciti tra quelli tassativamente previsti dal D.Lgs. 231/01;
- iv. coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187 *quater* TUF (D.Lgs. n. 58/1998).

c. Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale

L'Organismo di Vigilanza possiede, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite alla sua indipendenza, ne garantiscono l'obiettività di giudizio; all'interno dell'Organismo di Vigilanza sono presenti soggetti cumulativamente in possesso di professionalità adeguate in materia legale, economica, di controllo e gestione dei rischi aziendali. L'Organismo di Vigilanza può, inoltre, avvalersi di professionisti esterni dotati di specifiche competenze (come, ad esempio, quelle infortunistiche, di organizzazione aziendale, revisione, contabilità e finanza).

In particolare, l'OdV è in possesso di adeguate competenze specialistiche quali:

- conoscenza dell'organizzazione e dei principali processi aziendali tipici del settore in cui la Società opera;
- conoscenze giuridiche tali da consentire l'identificazione delle fattispecie suscettibili di configurare ipotesi di reato;
- capacità di individuazione e valutazione degli impatti, discendenti dal contesto normativo di riferimento, sulla realtà aziendale;
- conoscenza delle tecniche specialistiche proprie di chi svolge attività "ispettiva".

d. Continuità d'azione

L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza in merito alla corretta applicazione del Modello con adeguato impegno e con i necessari poteri di indagine. Ne cura inoltre l'attuazione assicurandone il costante aggiornamento.

L'OdV non svolge mansioni operative che possano condizionare e inficiare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

A tal riguardo:

- le attività poste in essere dall'OdV non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che l'Organo Dirigente vigila sull'adeguatezza del suo intervento, poiché ad esso compete la responsabilità ultima del funzionamento e dell'efficacia del Modello;
- l'OdV ha libero accesso presso tutte le funzioni di Lumagest (sia interne sia esternalizzate) – senza necessità di alcun consenso preventivo – al fine di ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal Decreto 231;
- l'OdV si può avvalere – sotto la sua diretta sorveglianza e responsabilità – dell'ausilio di tutte le strutture della Società ovvero, come sopra indicato, di Consulenti.

L'Organo Amministrativo valuta la sussistenza dei menzionati requisiti professionali e personali in capo ai suoi componenti. A tal riguardo, al momento della nomina dovranno essere forniti adeguate informazioni in merito alla presenza dei requisiti sopra indicati, anche allegando il *curriculum vitae* di ciascun componente al relativo verbale.

3.2 Funzione, poteri e compiti dell'Organismo di Vigilanza

All'OdV della Società è affidato il compito di:

- 1) vigilare sull'osservanza delle prescrizioni del Modello da parte dei Destinatari;
- 2) verificare l'idoneità e l'efficacia del Modello in relazione alla struttura della Società ed ai suoi eventuali mutamenti, nonché alla effettiva capacità di prevenire la commissione dei reati;
- 3) curare l'aggiornamento del Modello, in relazione alle mutate condizioni strutturali e alle novità legislative e giurisprudenziali.

Su di un piano più operativo è affidato all'OdV della Società il compito di:

- verificare l'efficienza ed efficacia del Modello organizzativo adottato ai sensi del D.Lgs. n. 231/2001;
- individuare e suggerire sistemi di controllo e monitoraggio tesi alla ragionevole prevenzione delle irregolarità ai sensi del D.Lgs. n. 231/2001;
- verificare il rispetto degli *standard* di comportamento e delle procedure previste dal Modello e rilevare gli eventuali scostamenti comportamentali, mediante analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni aziendali; per lo svolgimento delle attività verifica e di controllo, di

cui al presente punto e dei precedenti l'OdV, potrà avvalersi – come sopra indicato – delle attività di verifica delle funzioni di controllo;

- riferire periodicamente all'Organo Amministrativo e al Collegio Sindacale ove nominato (con periodicità non superiore a sei mesi), circa lo stato di attuazione e l'operatività del Modello;
- promuovere e/o sviluppare, di concerto con le funzioni aziendali a ciò preposte, programmi di informazione e comunicazione interna, con riferimento al Modello, agli *standard* di comportamento e alle procedure adottate ai sensi del D.Lgs. n. 231/2001;
- promuovere e/o sviluppare l'organizzazione, di concerto con le funzioni aziendali preposte, di corsi di formazione e la predisposizione di materiale informativo utili alla comunicazione e divulgazione dei principi etici e degli standard cui la Società si ispira nello svolgimento delle proprie attività;
- fornire chiarimenti in merito al significato e all'applicazione delle previsioni contenute nel Modello;
- assicurare l'aggiornamento del sistema di identificazione, mappatura e classificazione delle Attività Sensibili;
- raccogliere, elaborare e conservare le informazioni, comprese le segnalazioni, rilevanti in merito al rispetto del Modello;
- effettuare periodicamente verifiche ed ispezioni (anche a sorpresa) mirate su determinate operazioni e atti specifici, posti in essere nelle aree a rischio come individuate nel presente Modello; a tal proposito, l'OdV predispose un piano della propria attività su base annuale che sarà comunicato preventivamente all'Organo Amministrativo e al Collegio Sindacale ove nominato ed è dotato di un generale potere ispettivo avendo libero accesso senza la necessità di alcun consenso preventivo, salvo i casi in cui tale consenso sia reso necessario dalla legge o da regolamenti, a tutta la documentazione aziendale, con possibilità di acquisire dati e informazioni dai soggetti responsabili;
- segnalare all'organo amministrativo, per gli opportuni provvedimenti, quelle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;

- formulare proposte all'organo amministrativo e/o alle funzioni interessate, di eventuali aggiornamenti e adeguamenti del Modello organizzativo adottato e dei suoi elementi costitutivi, in conseguenza di:
 - significative violazioni delle prescrizioni del Modello;
 - significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
 - modifiche nello svolgimento delle attività aziendali;
 - modifiche normative;
- curare, in caso di controlli, ispezioni, richieste di informazioni da parte di autorità competenti finalizzati a verificare la rispondenza del Modello alle previsioni del D.Lgs. n. 231/2001, il rapporto con i soggetti incaricati dell'attività ispettiva fornendo loro adeguato supporto informativo;
- introdurre, se necessario e fermo restando quanto previsto nel presente documento, altre regole operative relative, ad esempio, alla cadenza delle proprie riunioni, alle eventuali specifiche mansioni affidate ai singoli componenti ovvero alla gestione delle informazioni acquisite nell'esercizio dell'incarico.
- indicare quali correzioni e modifiche si rende utile apportare alle procedure aziendali.

Tutte le attività poste in essere dall'OdV, nello svolgimento dei suoi compiti, non sono soggette al sindacato di alcun altro organismo o struttura della Società, fermo restando il potere di vigilanza sull'adeguatezza del suo operato affidato all'Organo Amministrativo, cui risale la responsabilità ultima dell'osservanza degli obblighi derivanti dal D.Lgs. n. 231/2001.

Per tutto ciò che attiene al funzionamento dell'OdV si fa rinvio al Regolamento dal medesimo organo.

3.3 Reporting dell'OdV nei confronti degli Organi Sociali

L'Organismo di Vigilanza informerà l'Organo Amministrativo e il Collegio Sindacale ove nominato in ordine all'attività svolta:

- mediante relazioni almeno annuali;
- ogniqualvolta se ne presenti e ravvisi la necessità e/o opportunità.

Le suddette relazioni dovranno contenere, oltre al resoconto dell'attività svolta, anche

l'indicazione delle eventuali criticità riscontrate e gli interventi correttivi e migliorativi pianificati, nonché il loro stato di realizzazione.

L'OdV potrà essere convocato in qualsiasi momento dall'Organo Amministrativo e dal Collegio Sindacale ove nominato o potrà a sua volta fare richiesta in tal senso per riferire in merito al funzionamento del Modello.

Di ogni adunanza dell'OdV con l'Organo Amministrativo e/o il Collegio Sindacale dovrà rimanere evidenza scritta, debitamente conservata.

3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza

L'art. 6, 2° comma, lett. d) del Decreto 231 impone la previsione nel Modello di obblighi informativi nei confronti dell'OdV deputato a vigilare sul funzionamento e l'osservanza del Modello stesso. L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto 231.

L'efficacia dell'attività di vigilanza trova fondamento in un sistema strutturato di flussi informativi provenienti da tutti i Destinatari del Modello, con riferimento a tutti gli atti, comportamenti od eventi, di cui vengano a conoscenza, che potrebbero determinare una violazione del Modello o che, più in generale, siano potenzialmente rilevanti ai fini del Decreto 231.

I flussi informativi nei confronti dell'Organismo di Vigilanza, fanno riferimento alle seguenti categorie di informazioni:

- informativa costante;
- informativa periodica.

Al fine di facilitare i flussi informativi verso l'OdV, è stata istituita una casella *e-mail* dell'Organismo di Vigilanza: [odvlumagest@citygreenlight.com].

Per quanto riguarda, invece, le segnalazioni in buona fede di violazioni del Modello e/o illeciti rilevanti ai sensi del Decreto 231 si rinvia al successivo paragrafo sul *whistleblowing*.

3.4.1. Informativa costante

Oltre alle notizie di cui al paragrafo precedente – che riguardano fatti o eventi di carattere eccezionale – dovranno altresì essere immediatamente comunicate all'Organismo di Vigilanza le informazioni rilevanti concernenti le seguenti attività ricorrenti:

- l'articolazione dei poteri e il sistema delle deleghe adottato dalla Società ed eventuali modifiche che intervengano sullo stesso;
- la documentazione relativa all'attività di informazione e formazione svolta in attuazione del Modello e alla partecipazione alla medesima da parte del personale (con indicazione di eventuali assenze ingiustificate);
- le relazioni e/o le verifiche predisposte dalle funzioni aziendali, anche di controllo;
- le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del modello organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le modifiche organizzative ivi comprese le modifiche/integrazioni delle procedure interne;
- la corrispondenza rilevante con gli *Outsourcer*;
- eventuale reportistica in materia di salute e sicurezza sul lavoro;
- qualsiasi incarico conferito alla società di revisione o a società ad esse collegate, diverso da quello concernente la revisione del bilancio.

3.4.2. Informativa periodica

Oltre alle notizie di cui al paragrafo precedente – che riguardano fatti o eventi di carattere eccezionale – dovranno, altresì, essere comunicate all'Organismo di Vigilanza su base periodica, le informazioni rilevanti al fine di agevolare l'opportuna attività di controllo secondo quanto richiesto dall'OdV e riportato nelle singole Parti Speciali del Modello.

3.5 Whistleblowing

Lumagest ha implementato un sistema di segnalazione interna per l'effettuazione delle segnalazioni, il divieto di ritorsione e un sistema disciplinare conformi al D.Lgs. 24/2023 di attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, *“riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione europea e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali?”* (“**Decreto Whistleblowing**”).

Il destinatario delle segnalazioni è individuato nell'Organismo di Vigilanza, che risulta appositamente formato in materia di *whistleblowing*.

Le segnalazioni relative alle violazioni del Modello o illeciti rilevanti ai sensi del Decreto 231

possono essere trasmesse da tutti i Destinatari (e da altri possibili segnalanti individuati dal Decreto *Whistleblowing*): **(i)** all'indirizzo *e-mail* dell'Organismo di Vigilanza (odvlumagest@citygreenlight.com); **(ii)** per posta all'indirizzo "Organismo di Vigilanza ex D.Lgs. 231/2001, Lumagest S.r.l., Via Giuseppe Zampieri, 15, 36100, Vicenza" attraverso l'invio o il deposito di n. 3 buste separate: la prima con i dati identificativi del segnalante e copia di un documento di riconoscimento; la seconda con il testo della segnalazione; la terza contenente le prime due e recante all'esterno la dicitura "riservata all'OdV"); **(iii)** *de visu* all'Organismo di Vigilanza tramite incontro di persona.

Qualunque sia il canale interno utilizzato, il segnalante deve specificare che quanto trasmesso è una "segnalazione *whistleblowing*" e se quanto segnalato rientra effettivamente nell'ambito applicativo del Decreto *Whistleblowing*, la segnalazione viene gestita in conformità a tale decreto.

Fatto salvo il caso di segnalazione anonima, in caso di segnalazione conforme al Decreto *Whistleblowing*, l'OdV svolge le seguenti attività:

- a. rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
- b. mantiene le interlocuzioni con la persona segnalante e può – laddove necessario – richiedere a quest'ultima integrazioni;
- c. dà diligente seguito alle segnalazioni ricevute;
- d. fornisce riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine dei sette giorni dalla presentazione della segnalazione.

Nell'ambito delle indagini relativi a una segnalazione, l'OdV si può avvalere di soggetti terzi nel rispetto degli obblighi di riservatezza previsti dal Decreto *Whistleblowing*.

Chi gestisce la segnalazione può, inoltre, sentire il segnalato anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

In caso di segnalazione effettuata oralmente nel corso di un incontro di persona tra il segnalante e l'OdV, quest'ultimo documenta la segnalazione, previo consenso del segnalante, tramite registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale, poi sottoscritto dal segnalante.

I segnalanti non possono subire alcuna ritorsione e, a tal proposito, il Decreto *Whistleblowing* dispone la previsione di misure di sostegno per i segnalanti e per altri soggetti espressamente

individuati dalla norma nonché la possibilità di comunicare all'ANAC le ritorsioni che ritengono di aver subito in ragione di una segnalazione.

In ogni caso, la Società adotta tutte le misure necessarie per garantire che sia assicurato il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

3.6 Obblighi di riservatezza

I componenti dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a operazioni strategiche della Società o a presunte violazioni del Modello.

I componenti dell'OdV si astengono altresì dall'utilizzare informazioni riservate per fini diversi da quelli di cui ai precedenti paragrafi e comunque per scopi non conformi alle funzioni di vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

3.7 Raccolta e conservazione delle informazioni.

Ogni informazione raccolta e ogni *report* ricevuto o preparato dall'Organismo di Vigilanza è conservato per 10 anni (o, nei casi di conservazione di documenti inerenti a una segnalazione ai sensi della normativa in materia di *whistleblowing*, per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni) in un apposito archivio tenuto dall'OdV in formato cartaceo o elettronico.

CAPITOLO 4

FORMAZIONE E DIFFUSIONE DEL MODELLO

4.1 Formazione ed informazione dei Dipendenti

Ai fini dell'efficacia del presente Modello, è obiettivo della Società garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei Destinatari, sia già presenti in azienda sia da inserire in futuro. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Attività Sensibili.

La comunicazione iniziale

Qualora Lumagest dovesse procedere ad assunzioni, ai soggetti assunti verrebbe consegnato un set informativo, al fine di assicurare agli stessi le conoscenze considerate di primaria rilevanza. Tale documentazione informativa dovrà contenere, oltre ai documenti di regola consegnati al neo-assunto, il Modello della Società. Tali soggetti saranno tenuti a rilasciare alla Società una dichiarazione sottoscritta ove si attesti la ricezione della documentazione informativa nonché la integrale conoscenza dei documenti allegati e l'impegno ad osservarne le prescrizioni.

La formazione

L'attività di formazione, volta a diffondere la conoscenza del Modello, è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società. Tutti i programmi di formazione avranno un contenuto minimo comune consistente nell'illustrazione dei principi del Decreto 231, degli elementi costitutivi il Modello, delle singole fattispecie di Reati presupposto e dei comportamenti considerati sensibili in relazione al compimento di detti reati.

In aggiunta a questa matrice comune, ogni programma di formazione sarà modulato al fine di fornire ai suoi fruitori gli strumenti necessari per il pieno rispetto del dettato del Decreto in relazione all'ambito di operatività ed alle mansioni dei soggetti destinatari del programma stesso.

All'interno dei piani di formazione previsti dalla Società, è inserita anche la formazione in materia di *whistleblowing*.

La partecipazione ai programmi di formazione sopra descritti è obbligatoria ed il controllo circa l'effettiva frequenza è demandato all'OdV.

La mancata partecipazione non giustificata ai programmi di formazione può comportare l'irrogazione di una sanzione disciplinare che sarà irrogata secondo le regole indicate nel Capitolo 7 del presente Modello.

4.2 Selezione e Informazione dei Consulenti, degli *Outsourcer*, dei Fornitori e delle controparti contrattuali della Società

I Consulenti, gli *Outsourcer*, i Fornitori e le controparti contrattuali della Società già esistenti al momento dell'adozione del Modello, devono essere informati di tale adozione e dell'esigenza di Lumagest che il loro comportamento sia conforme alle disposizioni del Modello stesso e non metta a rischio Lumagest di incorrere in responsabilità *ex D. Lgs. 231/2001*.

In occasione dell'instaurarsi di un nuovo rapporto con nuovi Consulenti, *Outsourcer* e Fornitori, la Società:

- a. informerà la controparte in merito al proprio impegno a svolgere la propria attività aziendale in modo lecito e nel pieno rispetto dei principi previsti dal Modello;
- b. chiederà alla controparte di tenere, a sua volta, condotte conformi ai principi del Modello;
- c. prevederà l'obbligo di informare la Società di qualsiasi atto o fatto, verificatosi nell'ambito delle attività aziendali compiute nell'interesse o vantaggio di Lumagest, che possa configurare un reato di cui al D.Lgs. 231/2001, nonché l'obbligo di comunicare qualsiasi coinvolgimento in procedimenti *ex D.Lgs. 231/2001* o la condanna per reati di cui al medesimo Decreto 231;
- d. si riserverà il diritto di risolvere il rapporto nel caso in cui la controparte sia indagata o condannata ai sensi del D.Lgs. 231/2001 per il compimento di Reati *ivi* previsti.

CAPITOLO 5

SISTEMA SANZIONATORIO

5.1 Funzione del sistema sanzionatorio

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di deterrenza) applicabili in caso di violazione delle regole di cui al presente Modello, rende efficiente l'azione di vigilanza dell'OdV ed ha lo scopo di garantire l'effettività del Modello stesso. La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'art. 6, comma 1, lettera e), D.Lgs. n. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità dell'ente.

L'applicazione del sistema sanzionatorio presuppone la semplice violazione delle disposizioni del Modello; pertanto, essa verrà attivata indipendentemente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto 231.

In virtù di quanto previsto dal sopra citato Decreto *Whistleblowing* e con riferimento a qualunque destinatario del Modello, si precisa che tra le condotte passibili di sanzione devono essere considerate anche la violazione, in qualsiasi modo, delle misure a tutela del segnalante, nonché l'effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate.

5.2 Sistema sanzionatorio dei Dipendenti

La violazione da parte dei Dipendenti soggetti al CCNL delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.

A. Dipendenti che non rivestono la qualifica di dirigenti

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori – nel rispetto delle procedure previste dall'art. 7, legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e delle eventuali normative speciali applicabili – sono quelli previsti dall'apparato sanzionatorio di cui al CCNL e precisamente:

- richiamo verbale;
- ammonizione scritta;
- multa (nei limiti stabiliti dal CCNL e da eventuali accordi sindacali tempo per tempo vigenti);

- sospensione dal lavoro e dal trattamento economico (nei limiti stabiliti dal CCNL e da eventuali accordi sindacali aziendali tempo per tempo vigenti);
- licenziamento (nei casi previsti dalla legge nonché in quelli previsti dal CCNL e da eventuali accordi sindacali aziendali tempo per tempo vigenti).

Restano ferme – e si intendono qui richiamate – tutte le disposizioni, previste dalla legge e dal CCNL applicato, relative alle procedure e agli obblighi da osservare nell'applicazione delle sanzioni.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli organi sociali e funzioni aziendali competenti.

Fermi restando gli obblighi per la Società, scaturenti dallo Statuto dei Lavoratori e dal CCNL applicabile, i comportamenti sanzionabili che costituiscono violazione del presente del Modello sono i seguenti:

- a) adozione, nell'espletamento delle Attività Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tali da determinare la concreta applicazione a carico della Società di sanzioni previste dal D.Lgs. 231/2001;
- b) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello;
- c) comportamenti che integrano violazioni previste dal Decreto *Whistleblowing*.

B. Dipendenti che rivestono la qualifica di dirigenti

In caso di violazione, da parte di dirigenti, del presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di un comportamento non conforme alle prescrizioni dello stesso, ovvero di violazioni previste dal Decreto *Whistleblowing*, la Società provvederebbe ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto normativamente previsto e in conformità con quanto previsto dal CCNL applicabile.

Più in particolare, in relazione alla gravità del comportamento commesso, potranno essere comminate le seguenti sanzioni.

- richiamo verbale da parte dell'Organo Amministrativo, per le ipotesi in cui il dirigente non si sia attenuto scrupolosamente alle indicazioni contenute nel presente Modello;

- richiamo scritto, per le ipotesi di maggior gravità rispetto a quelle di cui al punto precedente con comunicazione da parte dell'Organo Amministrativo;
- licenziamento per le ipotesi di gravità tale da non suggerire la prosecuzione del rapporto, con decisione assunta dall'Organo Amministrativo o da persona dallo stesso delegata.

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità e autonomia del dipendente e del dirigente, all'eventuale esistenza di precedenti disciplinari a carico del dipendente, all'intenzionalità del comportamento nonché alla gravità del medesimo (a titolo esemplificativo, nell'ipotesi di segnalazione di lieve entità avente ad oggetto la mancata partecipazione di un dipendente ad attività formativa in materia 231, seguirà un richiamo verbale ovvero in caso di mancata segnalazione o segnalazione mendace riguardante la commissione da parte di un altro dipendente di un reato ex Decreto 231 si potrà giungere fino al licenziamento), con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta – ai sensi e per gli effetti del Decreto 231 – a seguito della condanna censurata.

5.3 Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte degli Amministratori, ovvero di violazioni previste dal Decreto *Whistleblowing*, l'OdV informa l'intero Collegio Sindacale (ove nominato) e l'intero Organo Amministrativo i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea al fine di adottare le misure più idonee previste dalla legge e/o la revoca di deleghe eventualmente conferite all'Amministratore.

5.4 Misure nei confronti dei Sindaci (ove nominati)

In caso di violazione del Modello da parte di uno o più Sindaci di Lumagest, ovvero di violazioni previste dal Decreto *Whistleblowing*, l'OdV informa l'intero Collegio Sindacale e l'Organo Amministrativo i quali prenderanno le opportune iniziative previste dalla vigente normativa.

5.5 Misure nei confronti dei Consulenti, degli *Outsourcer*, dei Fornitori e delle controparti contrattuali della Società

Al fine di formalizzare l'impegno al rispetto dei principi del Modello e del Codice Etico da parte di terzi aventi rapporti contrattuali con la Società, è previsto l'inserimento nel contratto

di riferimento di un'apposita clausola, ovvero per i contratti già in essere, la sottoscrizione di una specifica pattuizione integrativa in tal senso.

Nell'ambito di tali clausole e pattuizioni, sono anche previste apposite sanzioni di natura contrattuale per l'ipotesi di violazione del Modello.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come – a titolo esemplificativo – nel caso di applicazione alla stessa da parte del giudice delle misure sanzionatorie previste dal Decreto 231.

PARTI SPECIALI

**PARTE SPECIALE – A – REATI COMMESSI NEI RAPPORTI CON LA
PUBBLICA AMMINISTRAZIONE**

**INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE
DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA**

CAPITOLO B.1

LE FATTISPECIE DI REATO

Le fattispecie dei reati nei rapporti con la P.A. (artt. 24 e 25, D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la P.A. Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel Decreto 231 agli artt. 24, 25 e 25 *decies*.

MALVERSAZIONE DI EROGAZIONI PUBBLICHE (ART. 316 *BIS* C.P.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti, sovvenzioni o contributi da parte dello Stato o di altro Ente Pubblico italiano o dell'Unione europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate. La condotta consiste nella mancata destinazione delle somme ottenute alle finalità per le quali erano state erogate.

INDEBITA PERCEZIONE DI EROGAZIONI PUBBLICHE (ART. 316 *TERC* 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 attestanti cose non vere ovvero mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea.

La pena è aumentata quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.

CONCUSSIONE (ART. 317 C.P.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della propria qualità o dei propri poteri, costringa taluno a dare o a promettere indebitamente a sé o ad altri denaro o altre utilità. Soggetto attivo del reato è il pubblico ufficiale o incaricato di un pubblico servizio (non il privato che subisca la costrizione proveniente dal soggetto pubblico).

CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE (c.d. corruzione impropria) E CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO (c.d. corruzione propria) (ARTT. 318 E 319 C.P.)

Tali ipotesi di reato si configurano nel caso in cui un pubblico ufficiale (o un incaricato di pubblico servizio, come prevede l'art. 320 c.p.) riceva o accetti la promessa, per sé o per altri,

di denaro o altra utilità per esercitare le sue funzioni o i suoi poteri (c.d. corruzione impropria) ovvero per omettere o ritardare un atto del suo ufficio o compiere un atto contrario al suo dovere d'ufficio (c.d. corruzione propria).

L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: lo svolgimento di una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: l'aggiudicazione di una gara ad un soggetto immeritevole, privo dei necessari requisiti di aggiudicazione).

Tali ipotesi di reato si differenziano dalla concussione, in quanto tra corrotto e corruttore esiste un accordo, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

L'art. 319 *bis* c.p. prevede che la pena sia aumentata se il fatto di cui all'art. 319 c.p. abbia per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

CORRUZIONE IN ATTI GIUDIZIARI (ART. 319 *TER* C.P.)

Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario (processo civile, amministrativo o penale) si corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART. 319 *QUATER* C.P.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della propria qualità o poteri, induca taluno a dare o promettere indebitamente, a lui o ad un terzo, denaro o altra utilità.

La pena è aumentata quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.

In questo caso (e a differenza della fattispecie di "Concussione") la punibilità, oltre che per il pubblico ufficiale e l'incaricato di pubblico servizio, è prevista anche per il soggetto privato, indotto a dare o promettere l'utilità indebita. In questo caso, infatti, il soggetto privato non subisce una "costrizione" e, pertanto, conserva una possibilità di scelta tra aderire o non aderire all'induzione indebita proveniente dal soggetto pubblico.

CORRUZIONE DI PERSONA INCARICATA DI UN PUBBLICO SERVIZIO (ART. 320 C.P.)

Ai sensi di tale norma, le fattispecie di corruzione (impropria e propria, artt. 318 e 319 c.p.) si applicano (non solo al soggetto che sia pubblico ufficiale, ma anche) a chi sia incaricato di pubblico servizio.

PENE PER IL CORRUTTORE (ART. 321 C.P.)

La disposizione prevede che le pene stabilite dagli articoli precedenti (corruzione impropria, corruzione propria, corruzione in atti giudiziari, induzione indebita) si applicano anche al soggetto privato, ossia a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.

ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso denaro o altra utilità ad un pubblico ufficiale o incaricato di pubblico servizio (per l'esercizio delle sue funzioni o dei suoi poteri o per indurlo a omettere o ritardare un atto del suo ufficio ovvero a compiere un atto contrario ai doveri del suo ufficio) e tale offerta o promessa non venga accettata.

PECULATO, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ, CORRUZIONE E ISTIGAZIONE ALLA CORRUZIONE, ABUSO D'UFFICIO, DI MEMBRI DELLE CORTI INTERNAZIONALI O DEGLI ORGANI DELLE COMUNITÀ EUROPEE O DI ASSEMBLEE PARLAMENTARI INTERNAZIONALI O DI ORGANIZZAZIONI INTERNAZIONALI E DI FUNZIONARI DELLE COMUNITÀ EUROPEE E DI STATI ESTERI (ART. 322 *BIS* C.P.)

Sulla base del richiamo all'art. 322-*bis* c.p. operato dall'art. 25 del Decreto, le fattispecie di reato di previste, tra gli altri, dagli articoli da 317 a 320 e 322, terzo e quarto comma, 323, c.p. si configurano anche nel caso in cui il denaro o altra utilità siano dati, offerti o promessi, anche a seguito di induzione a farlo:

- 1) ai membri della Commissione dell'Unione europea, del Parlamento dell'Unione europea, della Corte di Giustizia e della Corte dei conti dell'Unione europea;
- 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari dell'Unione europea o del regime applicabile agli agenti dell'Unione europea;
- 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso l'Unione europea, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti dell'Unione europea;

- 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono l'Unione europea;
- 5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
5-*bis*) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale.
5-*ter*) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;
5-*quater*) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;
5-*quinq*ues) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione.

Le disposizioni degli articoli 319-*quater*, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

- 1) alle persone indicate nel primo comma del presente articolo;
- 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

TRAFFICO DI INFLUENZE ILLECITE (ART. 346 *BIS* C.P.)

La norma in parola prevede la punizione di chiunque, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o con un incaricato di un pubblico servizio o con uno degli altri soggetti di cui all'art. 322 *bis* c.p., indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'art. 322 *bis* c.p. ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

Oltre al c.d. trafficante di influenze, è punito anche il soggetto che indebitamente dà o promette denaro o altra utilità al c.d. trafficante.

TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640, COMMA 2 N. 1, C.P.)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato, ad altro ente pubblico o all'Unione europea.

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 (i.e. contributi, sovvenzioni, finanziamenti, mutui agevolati).

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 in qualsiasi modo il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro Ente Pubblico.

FRODE NELLE PUBBLICHE FORNITURE (ART. 356 C.P.)

Tale ipotesi di reato si configura nei casi in cui chiunque commetta frode nell'esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali derivanti da un contratto di fornitura concluso con lo Stato, con un altro ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità.

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377 BIS C.P.)

La previsione di cui all'art. 377 *bis* c.p. intende sanzionare ogni comportamento diretto ad indurre – con violenza, minaccia o promessa di denaro o altra utilità – a non rendere dichiarazioni o a rendere dichiarazioni false una persona chiamata a rendere dichiarazioni dinanzi all'Autorità Giudiziaria nell'ambito di un procedimento penale e che potrebbe avvalersi della facoltà di non rispondere.

Tale interferenza sulle dichiarazioni altrui potrebbe essere finalizzata a celare elementi “compromettenti” a carico di un determinato ente, con evidente interesse del medesimo.

La norma mira a tutelare il corretto svolgimento dell'attività processuale contro ogni forma di indebita interferenza.

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti, sia correnti sia in occasione di eventi straordinari, con la Pubblica Amministrazione (ricomprendendo in tale definizione anche gli enti pubblici e le pubbliche amministrazioni straniere).

CAPITOLO B.1

CRITERI PER LA DEFINIZIONE DI P.A. E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo dai soggetti di cui all'art. 5, comma 1, lett. *a e b*, D.Lgs. n. 231/2001. Sono, inoltre, riportate anche indicazioni in merito alle fattispecie di reato che si possono compiere in relazione alle diverse categorie di soggetti coinvolti.

A.2.1 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. n. 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 (quali, ad esempio, 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, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, CONSIP, COVIP, Direzioni territoriali del lavoro, sezioni fallimentari);
- Regioni;
- Province;

- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, ISTAT, ENASARCO);
- ASL o ATS;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio, la RAI);
- Autorità doganali;
- Autorità di Vigilanza (quali ad esempio Banca d'Italia, Consob, IVASS);
- Fondazioni di previdenza ed assistenza;
- Soprintendenze.

Anche i soggetti di diritto privato concessionari di pubblici servizi e le società partecipate a maggioranza da un ente pubblico sono considerate, dalla più recente giurisprudenza, alla stessa stregua di enti pubblici.

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 possono configurare le fattispecie criminose *ex* D.Lgs. n. 231/2001.

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

A.2.2 Pubblici Ufficiali

Ai sensi dell’art. 357, primo comma, c.p., è considerato pubblico ufficiale “*agli effetti della legge penale*” chi esercita “*una pubblica funzione legislativa, giudiziaria o amministrativa*”.

Il secondo comma dell’Articolo in parola fornisce poi la nozione di “pubblica funzione amministrativa”. Non si è compiuta, invece, un’analoga attività definitoria per precisare le nozioni di “funzione legislativa” e “funzione giudiziaria”.

Il secondo comma dell’art. 357 c.p. 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 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.

Inoltre, il secondo comma dell’art. 357 c.p. traduce 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: (a) poteri deliberativi; (b) poteri autoritativi; (c) poteri certificativi.

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.

A.2.3 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 spiega 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 – così come per la “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.

Esempi di incaricati di pubblico servizio sono: i dipendenti delle Autorità di vigilanza che non concorrono a formare la volontà dell’autorità e che non hanno poteri autoritativi, i dipendenti

degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, ecc.

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.

È dunque stata indicata 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:

- (a) 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;
- (b) la presenza di una convenzione e/o concessione con la pubblica amministrazione;
- (c) l’apporto finanziario da parte dello Stato;
- (d) l’immanenza dell’interesse pubblico in seno all’attività economica.

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

CAPITOLO B.1

A.3.1 Attività Sensibili in relazione ai reati nei rapporti con la P.A. e al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

1. gestione dei rapporti correnti con enti pubblici e pubblici funzionari (ivi compresa la gestione di eventuali ispezioni);
2. partecipazione a gare pubbliche ed esecuzione di commesse pubbliche;
3. gestione dei contenziosi;
4. gestione dei procedimenti volti all'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o dell'Unione europea e loro impiego.

A.3.2 Attività Strumentali alla commissione di reati nei rapporti con la P.A. e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci

1. selezione dei Consulenti, dei Fornitori e degli *Outsourcer* e gestione dei relativi rapporti;
2. selezione e assunzione del personale;
3. omaggi, liberalità e sponsorizzazioni;
4. gestione delle spese di viaggio e di rappresentanza.

CAPITOLO B.1

REGOLE GENERALI

A.4.1 Il sistema in linea generale

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.

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, ai valori e alle politiche della Società e alle regole contenute nel presente Modello.

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

A.4.2 Il sistema di deleghe e procure

In linea di principio, il sistema di deleghe e procure della Società deve essere caratterizzato da elementi di “sicurezza” ai fini della prevenzione dei Reati (tracciabilità ed evidenza delle Attività Sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per “delega” l'atto interno di attribuzione di funzioni e compiti. Si intende per “procura” il negozio giuridico unilaterale con cui la 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 devono essere i seguenti:

- a) tutti coloro che intrattengono per conto della Società rapporti con la P.A. devono essere dotati di delega formale in tal senso;
- b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma aziendale ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- c) ciascuna delega deve definire in modo specifico ed inequivoco i poteri del delegato e il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
- d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;

- e) la delega prevede eventuali di poteri di spesa adeguati alle funzioni conferite al delegato.

I requisiti essenziali del sistema di attribuzione delle **procure**, ai fini di una efficace prevenzione dei Reati, sono i seguenti:

- a) le procure descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione aziendale che fissi: l'estensione di poteri di rappresentanza e gli eventuali limiti di spesa;
- b) le procure speciali devono dettagliatamente stabilire l'ambito di operatività e i poteri del procuratore;
- c) le procure devono essere tempestivamente aggiornate qualora si verifichi una di queste ipotesi: assunzione o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, ecc.

L'OdV verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza coi documenti interni all'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.

A.4.3 Principi generali di comportamento

I seguenti principi di carattere generale si applicano ai Destinatari del Modello sia direttamente che in forza di apposite clausole contrattuali.

È 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; sono, altresì, proibite le violazioni ai principi ed alle procedure aziendali eventualmente richiamate nella presente Parte Speciale.

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

- a) effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- b) offrire regali al di fuori di quanto previsto dalla prassi aziendale. In particolare, ai rappresentanti della P.A. italiane e straniere o a loro familiari non deve essere offerta, né direttamente né indirettamente, alcuna forma di regalo, doni o gratuite prestazioni che possano apparire, comunque, connessi con l'attività della Società o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società.

Anche in quei paesi in cui offrire regali o doni costituisce una prassi diffusa in segno di cortesia (ad esempio, regali natalizi), tali regali devono essere di natura appropriata e non contrastare con le disposizioni di legge e non devono, comunque, essere interpretati come richiesta di favori in contropartita, né superare il valore di Euro 150; gli omaggi e le regalie che – in via eccezionale – potranno essere ammessi dovranno essere preventivamente comunicati all’Organismo di Vigilanza e riportati in un apposito registro, all’interno del quale dovranno, altresì, essere indicati i soggetti terzi beneficiari nonché gli *iter* autorizzativi per l’elargizione degli stessi;

- c) accordare vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione italiani o stranieri che possano determinare le stesse conseguenze previste al precedente punto b);
- d) selezionare personale ovvero favorire l’avanzamento interno di carriera o il riconoscimento di premi o MBO per il raggiungimento di obiettivi a beneficio di taluni dipendenti, non ispirandosi a criteri strettamente meritocratici o in base a criteri di valutazione non oggettivi;
- e) riconoscere compensi o eseguire prestazioni in favore di Consulenti, agenti, intermediari, *Outsourcer* e i Fornitori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, del rapporto contrattuale costituito con gli stessi ed alle prassi vigenti in ambito locale;
- f) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati non dovuti;
- g) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati (ad esempio contributi per la formazione dei dipendenti);
- f) violare gli obblighi di natura negoziale concernenti pubbliche forniture.

CAPITOLO B.1

Principi specifici di comportamento

Ai fini dell'attuazione delle regole e divieti elencati al precedente Capitolo, devono rispettarsi i principi qui di seguito descritti.

1. Ai Destinatari del Modello che materialmente intrattengono rapporti con la P.A. per conto della Società deve essere formalmente conferito potere in tal senso (con apposita delega per gli eventuali Dipendenti e gli Organi Sociali ovvero nel relativo contratto di *outsourcing* o consulenza con *Outsourcer* e Consulenti). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica delega o procura scritta che rispetti tutti i criteri elencati al precedente Capitolo; in ogni caso, i Destinatari del Modello che materialmente intrattengono rapporti con la P.A. per conto della Società informano su base continuativa l'Organo Amministrativo e su base periodica l'OdV circa gli esiti degli incontri più rilevanti o critici con la P.A.;
2. i ruoli e le responsabilità delle funzioni interne coinvolte nella gestione delle gare pubbliche devono essere espressamente individuati; a tali soggetti compete, *inter alia*, (i) la definizione di tutti gli *step* necessari alla partecipazione ad una gara pubblica; (ii) la gestione dei rapporti con i *competitor* in tali situazioni; (iii) il controllo della documentazione prima dell'invio alla P.A.; (iv) la gestione di eventuali incontri con l'ente appaltante; (v) la gestione di una scheda di evidenza che dia traccia di ogni passaggio relativo all'*iter* di gara;
3. i ruoli e le responsabilità delle funzioni interne coinvolte nella gestione delle attività di esecuzione delle commesse pubbliche devono essere espressamente individuati;
4. nelle attività di esecuzione dei contratti con i soggetti pubblici si deve provvedere ad esplicitare correttamente gli adempimenti contrattuali e/o normativi ivi previsti, ponendo in essere adeguati presidi al fine di garantire che quanto previsto nel capitolato tecnico e nei contratti sottoscritti con i soggetti pubblici sia recepito correttamente nei processi di esecuzione;
5. nelle attività di esecuzione dei contratti con i soggetti pubblici sono previsti controlli e verifiche intermedi, volti a verificare la corretta esecuzione degli obblighi assunti con l'ente pubblico, affinché i beni e/o i servizi prestati corrispondano ai parametri di qualità e quantità indicati all'interno dei contratti e/o convenzioni stipulati con la P.A., garantendo la tracciabilità dei principali passaggi valutativi, autorizzativi e di comunicazione con le parti dell'intero processo;

6. i Consulenti, gli *Outsourcer* e i Fornitori devono essere scelti con metodi trasparenti e secondo specifica procedura (ad esempio utilizzando apposite *liste predefinite* di controparti di fiducia o una procedura formalizzata di *beauty contest*). Se si tratta del primo incarico, viene richiesta documentazione (eventualmente anche un'autocertificazione) comprovante il possesso dei requisiti di professionalità e onorabilità, con l'obbligo per gli stessi di comunicare senza ritardo l'eventuale venir meno di uno di detti requisiti (ad esempio, condanna per qualche reato o sanzione disciplinare dell'Ordine professionale di appartenenza in caso di Consulenti);
7. i contratti con i Consulenti, gli *Outsourcer* e i Fornitori devono essere definiti per iscritto in tutte le loro condizioni e termini e contenere: (i) clausole standard con cui i medesimi dichiarino di essere a conoscenza del Modello adottato dalla Società, di impegnarsi a rispettarlo per quanto loro applicabile, di aver eventualmente adottato anch'essi un analogo codice di comportamento o modello organizzativo e di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Modello e nel D.Lgs. n. 231/2001 (o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte della Società in caso si addivenga all'instaurazione del rapporto), (ii) apposite clausole che regolino le conseguenze della violazione da parte degli stessi delle norme di cui al Modello (clausole risolutive espresse e penali);
8. a tutti i Consulenti, *Outsourcer* e Fornitori che già svolgono attività o prestano servizi in favore della Società, verrà inviata apposita informativa al fine di (i) comunicare ai medesimi l'avvenuta adozione del Modello da parte della Società; (ii) invitare tali soggetti a prendere visione del Modello; (iii) ribadire l'impegno dei medesimi al rispetto dei contenuti del Modello;
9. le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi, finanziamenti, concessioni e licenze devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti;
10. in occasione di contenziosi in cui è interessata la Società, è fatto divieto ai Destinatari coinvolti di esibire documenti/dati falsi o alterati, rilasciare dichiarazioni false, sottrarre o omettere informazioni dovute al fine di orientare indebitamente a proprio favore le decisioni dell'organo giudicante;

11. in occasione di contenziosi in cui è interessata la Società, è fatto divieto di promettere denaro o altra utilità ad una persona chiamata a rendere testimonianza inducendola a non rendere dichiarazioni o a rendere dichiarazioni mendaci;
12. coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi ad attività quali il pagamento di fatture, la destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc., devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie;
13. alle ispezioni giudiziarie, tributarie e amministrative devono partecipare almeno due soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali. Nel caso il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta;
14. con riferimento alla gestione finanziaria, la Società attua specifici controlli comportamentali e cura con particolare attenzione i flussi che non rientrano nei processi tipici dell'azienda e che sono quindi gestiti in modo estemporaneo e discrezionale. La finalità di detti controlli è volta ad impedire la formazione di riserve occulte;
15. il processo di selezione del personale deve avvenire secondo criteri di trasparenza basati sui seguenti parametri: parità di trattamento tra i candidati, valorizzazione del merito, professionalità adeguata rispetto all'incarico o alle mansioni da assegnare, conservazione della documentazione relativa all'assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo;
16. tutta la corrispondenza con la P.A. deve essere adeguatamente archiviata e conservata;
17. in relazione ai rimborsi spesa, è vietato a tutti gli Esponenti Aziendali e ai Dipendenti di effettuare spese ingiustificate e che non rispettino le delibere dell'Organo Dirigente o le procedure interne;
18. la Società registra e conserva tutte le note spese di lavoro ed effettua controlli periodici sulle stesse al fine di far emergere eventuali atti di disposizione "anomali" delle disponibilità finanziarie della stessa;

19. la Società prevede specifici limiti e modalità al rimborso di spese anticipate da Esponenti Aziendali e Dipendenti per l'esercizio delle attività sociali, nonché l'esibizione di adeguati documenti giustificativi delle spese sostenute;
20. la Società registra tutti gli omaggi e le liberalità eventualmente riconosciuti dalla stessa a soggetti terzi e viceversa, gli omaggi e le liberalità ricevuti da parte di soggetti terzi.

CAPITOLO B.1

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella policy aziendali adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

È altresì attribuito all'OdV il potere di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

CAPITOLO B.1

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, i flussi informativi nei confronti dell'Organismo di Vigilanza devono avvenire secondo quanto previsto nella seguente tabella:

Soggetto	Oggetto	Periodicità
Amministratore Unico/CFO	Elenco e copia delle deleghe e procure rilasciate a Esponenti Aziendali, Dipendenti e/o Consulenti al fine di intrattenere rapporti con la Pubblica Amministrazione	Annuale
	Elenco delle ispezioni ricevute e/o in corso, specificando: i) Pubblica Amministrazione procedente; ii) soggetti partecipanti e iii) periodo di svolgimento. Trasmissione dei verbali d'ispezione che diano evidenza di criticità.	Ad evento
	Informativa relativa a eventuali criticità inerenti l'iter di partecipazione ad una gara pubblica ovvero l'eventuale aggiudicazione.	Ad evento
	Comunicazione dell'elargizione di omaggi o regalie nei confronti di soggetti terzi che superano il valore di Euro 150 ciascuna.	Ad evento
Legale	Informativa relativa ai contenziosi giudiziali ed extragiudiziali (che superano la soglia di valore di Euro 10.000).	Annuale
CFO	Elenco delle richieste di finanziamenti, contributi o altra forma di erogazione pubblica (incluse le erogazioni pubbliche erogate da enti e/o istituzioni dell'Unione europea).	Annuale
Amministrazione del Personale	Reporting periodico sull'acquisizione di nuovi Consulenti e Fornitori (in riferimento alla stipulazione	Annuale

	dei contratti la cui soglia di valore è ritenuta significativa dalla Società).	
Amministratore Unico	Informativa relativa a eventuali criticità inerenti l' <i>iter</i> di partecipazione a gare.	Ad evento

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

PARTE SPECIALE – B – REATI SOCIETARI

CAPITOLO B.1

LE FATTISPECIE DI REATO

Le fattispecie dei reati societari (art. 25 *ter*, D.Lgs. n. 231/2001)

FALSE COMUNICAZIONI SOCIALI (ART. 2621 C.C.)

FATTI DI LIEVE ENTITÀ (ART. 2621 BIS C.C.)

FALSE COMUNICAZIONI SOCIALI DELLE SOCIETÀ QUOTATE (ART. 2622 C.C.)

Gli artt. 2621, 2621-bis e 2622 del Codice Civile prevedono le fattispecie di reato di c.d. falso in bilancio.

L'ipotesi di reato di cui all'art. 2621 c.c. si configura nel caso in cui, al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti consapevolmente (ad opera di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori), nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero ovvero vengano omessi fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo ad indurre in errore i destinatari sulla predetta situazione. Il reato si configura anche qualora le falsità o le omissioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Ai sensi dell'art. 2621 bis c.c., inoltre, qualora i fatti richiamati al precedente art. 2621 c.c. costituiscano fatti di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta, troveranno applicazione pene in misura ridotta rispetto a quelle previste ai sensi dell'art. 2621 c.c. sopra indicato. Le predette pene troveranno applicazione altresì allorquando i fatti di cui all'articolo 2621 c.c. riguardino società che non superano i limiti indicati dal secondo comma dell'articolo 1 del Regio Decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

Il reato di c.d. falso in bilancio può essere integrato non soltanto attraverso la materiale alterazione di dati contabili ma anche attraverso una artificiosa valutazione di beni o valori indicati nelle comunicazioni sociali (c.d. falso valutativo); secondo la Giurisprudenza, il reato sussiste anche laddove: “in presenza di criteri di valutazione normativamente fissati o di criteri tecnici generalmente accettati, l'agente da tali criteri si discosti consapevolmente e senza darne

adeguata informazione giustificativa, in modo concretamente idoneo ad indurre in errore i destinatari delle comunicazioni”.

Soggetti attivi di tali reati sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori. Resta, tuttavia, la possibilità del concorso eventuale di persone nel reato, in virtù del quale potranno rispondere del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche coloro che non rivestano le predette qualifiche.

OMESSA COMUNICAZIONE DEL CONFLITTO DI INTERESSI (ART. 2629 BIS C.C.)

Tale ipotesi di reato consiste nella violazione degli obblighi previsti dall'art. 2391, primo comma c.c. da parte dell'amministratore o di un componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione siano derivati danni alla società o a terzi.

L'art. 2391, primo comma, c.c. impone agli amministratori delle società per azioni di dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata. Gli amministratori delegati devono altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale. L'organo amministrativo deve darne notizia anche alla prima assemblea utile.

INDEBITA RESTITUZIONE DEI CONFERIMENTI (ART. 2626 C.C.)

Il reato in questione, come quello previsto dal successivo art. 2627 c.c., riguarda la tutela dell'integrità del capitale sociale e si compie quando gli amministratori, in assenza di legittime ipotesi di riduzione del capitale sociale, provvedono a restituire, anche per equivalente, i conferimenti effettuati dai soci ovvero liberano i soci dall'obbligo di eseguirli. Il reato in esame assume rilievo solo quando, per effetto degli atti compiuti dagli amministratori, si intacca il capitale sociale e non i fondi o le riserve. Per questi ultimi, eventualmente, sarà applicabile il reato contemplato dal successivo art. 2627 c.c.

La indebita restituzione dei conferimenti può essere realizzata in modo palese (quando gli amministratori restituiscono beni ai soci senza incasso di alcun corrispettivo o rilasciano dichiarazioni dirette a liberare i soci dai loro obblighi, non adempiuti, di versamento) ovvero dissimulato (quando gli amministratori, per esempio, distribuiscono utili fittizi con somme

prelevate dal capitale sociale e non dalle riserve, oppure compensano il credito vantato dalla società con crediti inesistenti vantati da uno o più soci).

Soggetti attivi del reato possono essere solo gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE (ART. 2627 C.C.)

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di 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.

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è l'arresto fino ad un anno.

ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La norma è diretta alla tutela dell'effettività e integrità del capitale sociale e non può prescindere dall'analisi di cui all'art. 2357 c.c., a norma del quale la società per azioni non può acquistare azioni proprie, nemmeno tramite società fiduciaria o per interposta persona, se non nei limiti degli utili distribuibili o delle riserve disponibili risultanti dall'ultimo bilancio regolarmente approvato. La norma prevede che le azioni devono essere interamente liberate.

L'illecito potrà essere realizzato attraverso non solo il semplice acquisto di azioni, ma anche attraverso il trasferimento della proprietà delle azioni mediante permuta o contratti di riporto o senza corrispettivo, mediante ad esempio una donazione.

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori.

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

Soggetti attivi del reato sono gli amministratori. Resta, tuttavia, la possibilità del concorso eventuale di persone nel reato, in virtù del quale potranno rispondere del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche coloro che non rivestano le predette qualifiche.

FORMAZIONE FITTIZIA DEL CAPITALE (ART. 2632 C.C.)

Tale ipotesi di reato è integrata dalle seguenti condotte:

- a) formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;
- b) sottoscrizione reciproca di azioni o quote;
- c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori ed i soci conferenti. Resta, tuttavia, la possibilità del concorso eventuale di persone nel reato, in virtù del quale potranno rispondere del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche coloro che non rivestano le predette qualifiche.

IMPEDITO CONTROLLO (ART. 2625 C.C.)

Tale ipotesi di illecito consiste nell'impedire od ostacolare, mediante occultamento di documenti o con altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.

Soggetti attivi sono gli amministratori. Resta, tuttavia, la possibilità del concorso eventuale di persone, in virtù del quale potranno essere ritenuti responsabili anche coloro che non rivestano le predette qualifiche.

ILLECITA INFLUENZA SULL'ASSEMBLEA (ART. 2636 C.C.)

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Tra le condotte suscettibili di integrare il reato in questione si possono annoverare, ad esempio, l'ammissione al voto di soggetti non aventi diritto (perché, ad esempio, in conflitto di interessi con la delibera in votazione) o la falsa rappresentazione della presenza della maggioranza dei soci alle assemblee.

Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

AGGIOTAGGIO (ART. 2637 C.C.)

Tale ipotesi di reato consiste nel diffondere notizie false ovvero nel realizzare operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati (ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari).

Si pensi, ad esempio, al caso in cui vengano diffuse dalla Società degli studi su sé stessa con previsioni di dati esagerati e/o falsi.

Anche questa fattispecie è stata costruita come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (ART. 2638 C.C.)

Si tratta di un'ipotesi di reato che può essere realizzata con due ordini di condotte:

- il primo ordine di condotte è integrato da (i) l'esposizione nelle comunicazioni previste dalla legge alle autorità pubbliche di vigilanza, quali ad esempio Consob o Banca d'Italia, al fine di ostacolare l'esercizio delle funzioni di queste ultime, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione

economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) l'occultamento, con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria.

La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

In relazione a questo primo ordine di condotte, la responsabilità sussiste indipendentemente dal fatto che dalla condotta sia derivato un effettivo ostacolo alle funzioni dell'Autorità di Vigilanza.

- il secondo ordine di condotte può essere integrato “in qualsiasi forma, anche omettendo le comunicazioni dovute”, purché da tali condotte, che non necessariamente devono riguardare la situazione economica, patrimoniale o finanziaria dei soggetti vigilati, derivi un effettivo ostacolo alle funzioni di vigilanza.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci, i liquidatori o altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza. Resta, tuttavia, la possibilità del concorso eventuale di persone nel reato, in virtù del quale potranno rispondere del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche coloro che non rivestano le predette qualifiche.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è aumentata del doppio qualora si tratti 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'art. 116 TUF.

Agli effetti della legge penale, le autorità e le funzioni di risoluzione di cui al decreto di recepimento della direttiva 2014/59/UE sono equiparate alle autorità di vigilanza.

FALSE O OMESSE DICHIARAZIONI PER IL RILASCIO DEL CERTIFICATO PRELIMINARE (ART. 54, D.LGS. 19/2023)

Tale ipotesi di reato potrebbe essere commessa nell'ambito di un'operazione di fusione transfrontaliera effettuata dalla Società. In tale occasione, il reato potrebbe configurarsi laddove fossero alterati ovvero falsificati i documenti da presentare al notaio per il rilascio del certificato preliminare alla fusione oppure laddove fossero rese dichiarazioni false ovvero si omettesse di rendere al notaio informazioni rilevanti per il rilascio del suddetto certificato. Il fine è quello di far apparire adempite le condizioni previste dalla normativa per il rilascio del suddetto certificato.

Nello specifico, l'art. 29 del D.Lgs. 19/2023 prevede che, su richiesta della società italiana partecipante alla fusione transfrontaliera, il notaio rilasci il certificato preliminare attestante il regolare adempimento, in conformità alla legge, degli atti e delle formalità preliminari alla formalizzazione **della fusione**.

CAPITOLO B.2

B.2.1 Attività Sensibili nell'ambito dei Reati Societari

1. tenuta della contabilità, predisposizione di bilanci, relazioni, prospetti e comunicazioni sociali in genere previste dalla legge.

CAPITOLO B.3

REGOLE GENERALI

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati Societari, è che tutti i Destinatari del Modello si attengano – nei limiti delle rispettive competenze – a regole di condotta conformi a quanto qui prescritto oltre che nelle *policy* e procedure adottate dalla Società.

B.3.1 Il sistema in linea generale

Premesso che Lumagest ha adottato una serie di procedure specifiche per presidiare gli aspetti attinenti alla gestione sociale e che dette regole e procedure si intendono qui interamente richiamate, oltre alle regole di cui al presente Modello e, in particolare, a quelle indicate ai successivi paragrafi, i Dipendenti e gli Organi Sociali della Società devono in generale conoscere e rispettare:

1. le vigenti prassi e procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico–funzionale aziendale ed organizzativa ed il sistema di controllo della gestione che si intendono qui interamente richiamate;
2. le norme inerenti il sistema amministrativo, contabile, finanziario e di *reporting* esistenti;
3. la normativa applicabile.

B.3.2 Principi generali di comportamento

La presente Parte Speciale prevede l'esplicito divieto a carico dei Dipendenti, degli Organi Sociali, degli *Outsourcer* e dei Consulenti della Società 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*, D.Lgs. n. 231/2001) e che sebbene non costituiscano di per sé un'ipotesi di Reato Societario, possano esserne il presupposto (ad esempio, mancato controllo). Sono, altresì, proibite le violazioni ai principi ed alle procedure aziendali potenzialmente rilevanti ai fini della presente Parte Speciale.

A livello generale,

- tutte le comunicazioni sociali devono essere redatte in modo tale che siano determinati con chiarezza, verità e completezza i dati e le notizie che ciascuna funzione fornisce, i

criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili;

- la rilevazione dei dati di bilancio e la loro elaborazione ai fini della predisposizione della bozza di bilancio deve seguire i principi di veridicità, correttezza, precisione e completezza dei dati e delle informazioni contenute nel bilancio ovvero negli altri documenti contabili oltre che nei documenti a questi ultimi connessi;
- tutte le operazioni sul capitale sociale nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni (anche transfrontaliere) e le scissioni devono essere effettuate nel rispetto della normativa vigente.

CAPITOLO B.4

Principi specifici di comportamento

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi i principi specifici qui di seguito descritti.

È previsto l'obbligo a carico dei soggetti sopra indicati di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, delle prassi 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 ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
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 della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare nel rispetto delle leggi vigenti.

In generale, è fatto divieto di:

- 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 Società;
- c) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- d) ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- e) acquistare o sottoscrivere azioni della Società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;

- f) effettuare riduzioni del capitale sociale, fusioni (anche transfrontaliere) o scissioni in violazione delle disposizioni di legge applicabili, ivi incluse quelle a tutela dei creditori, provocando ad essi un danno;
- g) 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;
- h) 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 da parte del Collegio Sindacale (ove esistente);
- i) 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.

Si dispone, inoltre, l'attuazione dei seguenti presidi integrativi:

- previsione di riunioni periodiche tra Collegio Sindacale (ove esistente) e OdV per verificare l'osservanza della disciplina in tema di normativa societaria;
- trasmissione al Collegio Sindacale (ove esistente), con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del CdA o sui quali esso debba esprimere un parere ai sensi di legge.

Con riferimento agli aspetti relativi alla selezione e alla gestione dei rapporti con Consulenti, *Outsourcer* e Fornitori, si richiamano espressamente, in quanto applicabili, le regole già illustrate nella Parte Speciale A.

CAPITOLO B.5

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella policy aziendale adottata ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

CAPITOLO B.6

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, sono previsti i seguenti flussi informativi nei confronti dell'Organismo di Vigilanza:

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Amministratore Unico/CFO	Comunicazione delle seguenti informazioni: i) approvazione del bilancio ed eventuali modifiche intervenute in sede di assemblea rispetto al progetto di bilancio; ii) eventuali operazioni effettuate sul capitale nel periodo di riferimento; iii) possibili conflitti di interesse dichiarati dagli amministratori in relazione a determinate operazioni cui la Società partecipa; e iv) procedure e interventi organizzativi adottati al fine di garantire la tracciabilità dei flussi contabili e finanziari.	Annuale

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

**PARTE SPECIALE – C – REATI DI RICETTAZIONE, RICICLAGGIO E
IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA
ILLECITA, NONCHÉ AUTORICICLAGGIO E REATI CON FINALITÀ
DI TERRORISMO E DELITTI IN MATERIA DI STRUMENTI DI
PAGAMENTO DIVERSI DAI CONTANTI**

CAPITOLO C.1

Le fattispecie di reato

La presente Parte Speciale si riferisce rispettivamente ai Reati di Riciclaggio introdotti nel *corpus* del D.Lgs. 231/2001, all'art. 25 *octies*, ai Reati con finalità di terrorismo introdotti all'art. 25-*quater* del D.Lgs. 231/2001 e ai Delitti commessi con strumenti di pagamento diversi dai contanti introdotti all'art. 25-*octies*.1 del D.Lgs. 231/2001, tenuto conto dell'affinità dei presidi aziendali finalizzata alla prevenzione di entrambe le fattispecie.

I reati di Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-*octies*, D. Lgs. n. 231/2001)

Per Reati di Riciclaggio, considerati tali anche se le attività che hanno generato i beni da riciclare si sono svolte nel territorio di un altro Stato comunitario o di un Paese extracomunitario, si intendono:

Ricettazione (art. 648 c.p.)

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto o contravvenzione, o comunque si intromette nel farli acquistare, ricevere od occultare.

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

Per “ricezione” si intende ogni forma di conseguimento del possesso del bene proveniente dal delitto o contravvenzione, anche se solo temporaneamente.

Per “occultamento” si intende il nascondimento del bene proveniente da delitto dopo averlo ricevuto.

Perché sussista il reato non è necessario che il denaro o i beni debbano provenire direttamente o immediatamente da un qualsiasi reato, ma è sufficiente anche una provenienza mediata, a condizione che l'agente sia consapevole di tale provenienza. Ricorre pertanto il delitto in esame non solo in relazione al prodotto o al profitto del reato, ma anche al denaro o alle cose che costituiscono il prezzo del reato, cioè alle cose acquistate col denaro di provenienza delittuosa oppure al denaro conseguito dall'alienazione di cose della medesima provenienza (si pensi al caso in cui la Società, al fine di ottenere un prezzo vantaggioso, acquisti beni da un soggetto che, parallelamente alla fornitura di tali beni, notoriamente svolga attività illecite quali lo spaccio di stupefacenti o faccia parte di un'associazione di tipo mafioso e utilizzi i profitti derivanti da tali attività illecite per investirli nell'attività lecita).

Riciclaggio (art. 648 bis c.p.)

Tale ipotesi di reato si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto o contravvenzione, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Per “sostituzione” si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.

Per “trasferimento” si intende la condotta consistente nel ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali.

Per la realizzazione di tale reato, dunque, è richiesto un *quid pluris* rispetto al reato di ricettazione, ovvero il compimento di atti o fatti diretti alla sostituzione del denaro.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

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

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto o contravvenzione.

La punibilità per tale reato è prevista solo per coloro i quali non siano già compartecipi del reato principale ovvero non siano imputabili a titolo di ricettazione o riciclaggio.

Il termine “impiegare” è normalmente sinonimo di “utilizzo per qualsiasi scopo”: tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che per “impiegare” debba intendersi in realtà “investire”. Pertanto, dovrebbe ritenersi rilevante un utilizzo a fini di profitto.

Premesso che presupposto comune di tutte e tre le fattispecie incriminatrici di cui agli artt. 648, 648 *bis* e 648 *ter* c.p. è quello costituito dalla provenienza da delitto o contravvenzione del denaro o di qualsiasi altra utilità di cui l'agente sia venuto a disporre, si precisa che tali fattispecie si distinguono sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della su indicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda o la terza richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto alla terza, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche o finanziarie.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

Autoriciclaggio (Art. 648 ter.1 c.p.)

L'1 gennaio 2015 è entrata in vigore la Legge n. 186/2014 recante “*Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio*”.

Ai sensi dell'art. 3, comma 5 della Legge sopracitata, è stata estesa la responsabilità amministrativa degli enti di cui al Decreto 231 anche al Reato di Autoriciclaggio, attraverso l'inserimento nell'art. 25 *octies* del Decreto 231 di un richiamo espresso a tale fattispecie di reato.

Nel caso in cui il denaro, i beni o le altre utilità provengano da reato per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni, è prevista per l'ente l'applicazione di una sanzione più severa.

La norma in parola prevede la sanzione della reclusione da due a otto anni e la multa da Euro 5.000 a Euro 25.000 per chi, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Il secondo comma prevede la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Il terzo comma dell'art. 648 *ter.1* c.p. prevede, inoltre, un'altra circostanza attenuante se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni .

Tale previsione non si applica tuttavia nell'ipotesi in cui il suddetto reato sia stato commesso con le modalità di cui all'art. 416 *bis.1* c.p. concernente il reato di “*Circostanze aggravanti e attenuanti per i reati connessi ad attività mafiose*” ovvero al fine di agevolare l'attività delle associazioni di tipo mafioso, nel qual caso troveranno applicazione le pene previste dal primo comma dell'art. 648 *ter.1* c.p., costituendo tale circostanza un'aggravante (art. 648 *ter.1*, comma 3, c.p.).

Un'ulteriore circostanza aggravante è prevista al quinto comma del suddetto articolo, il quale prevede l'aumento della pena qualora i fatti siano commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

Costituisce invece una circostanza attenuante la condotta di colui il quale *“si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l’individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto”* (art. 648 *ter.1*, comma 6, c.p.).

In ogni caso, la condanna comporta, ai sensi dell’art. 648 *quater* c.p., la confisca dei beni che costituiscono il prodotto o il profitto del reato, salvo che appartengano a persone estranee allo stesso reato. Qualora detta confisca non sia possibile, il giudice potrà comunque disporre la confisca del denaro, dei beni o delle altre utilità delle quali il reo abbia la disponibilità, anche per interposta persona, per un valore equivalente al prodotto, profitto o prezzo del reato. In relazione al reato in esame, il pubblico ministero potrà compiere, a sua volta, ogni attività di indagine che si rendesse necessaria circa i beni, il denaro o le altre utilità da sottoporre a confisca.

Non è invece punibile, ai sensi del comma 4 del summenzionato art. 648 *ter.1* c.p., l’autore del Reato di Autoriciclaggio allorquando il denaro, i beni o le altre utilità vengano destinati *“alla mera utilizzazione o al godimento personale”*.

Si applica, altresì, l’ultimo comma dell’art. 648 c.p. relativo al reato di *“Ricettazione”* secondo cui *“le disposizioni di questo art. si applicano anche quando l’autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto”*.

I reati di finanziamento del terrorismo

Finanziamento del terrorismo

Il Reato di Finanziamento del Terrorismo è stato introdotto con il D.Lgs. 109/2007, di recepimento della direttiva 2005/60/CE emanata dal Parlamento europeo e dal Consiglio in data 26 ottobre 2005.

Per Finanziamento del Terrorismo si intende: *“qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all’intermediazione, al deposito, alla custodia o all’erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipendentemente dall’effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti”*.

La nuova normativa in tema di Finanziamento del Terrorismo adotta le medesime misure di prevenzione già vigenti contro i Reati di Riciclaggio ed introdotte con il Decreto Antiriciclaggio, prevedendo inoltre altre norme idonee per attuare il congelamento dei fondi

e delle risorse economiche disposto dalle numerose risoluzioni del Consiglio di sicurezza delle Nazioni Unite che si sono succedute dal 1999 ad oggi, dal Regolamento CE n. 2580/2001 emanato dal Consiglio in data 27 dicembre 2001 e relativo a misure restrittive specifiche destinate a combattere il terrorismo, nonché dai Regolamenti comunitari emanati ai sensi degli artt. 60 e 301 del Trattato istitutivo della Comunità europea per il contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale.

Il congelamento dei fondi e delle risorse economiche è disposto, con decreto, su proposta del Comitato di sicurezza finanziaria, dal Ministro dell'Economia e delle Finanze, di concerto con il Ministro degli Affari Esteri.

Ai sensi del D.Lgs. 109/2007, per “*congelamento di fondi*” si intende il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione del portafoglio. Per “*congelamento di risorse economiche*” si intende, invece, il divieto di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia.

I delitti in materia di strumenti di pagamento diversi dai contanti.

INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493-TER C.P.)

L'art. 493-ter c.p. punisce la condotta di chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abilita al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

Il primo comma della norma prevede che è, altresì, punito chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)

Ai sensi dell'art. 493-*quater* c.p., è punito, salvo che il fatto costituisca più grave reato, chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

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

Si configura il reato di frode informatica quando, procurando a sé o ad altri un ingiusto profitto con altrui danno, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico.

Il reato di frode informatica è richiamato dall'art. 25-*octies.1* con riferimento alla sola ipotesi aggravata di cui al secondo comma dell'art. 640-*ter* c.p. (“*se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema*”).

CAPITOLO C.2

C.2.1 Attività Sensibili nell'ambito dei Reati di Ricettazione, Riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché Autoriciclaggio e dei Reati con finalità di Terrorismo e Delitti in materia di strumenti di pagamento diversi dai contanti

1. predisposizione delle dichiarazioni fiscali e gestione degli adempimenti fiscali (gestione della fiscalità aziendale);
2. attività di investimento;
3. donazioni e sponsorizzazioni;
4. selezione dei Fornitori e gestione degli acquisti;
5. gestione di strumenti di pagamento diversi dai contanti.

CAPITOLO C.3

REGOLE GENERALI

C.3.1 Principi generali di comportamento

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati nella stessa considerati, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e ai principi che siano direttamente o indirettamente funzionali alla prevenzione del fenomeno del riciclaggio adottati dalla Società come presidio fondamentale per il buon funzionamento, l'affidabilità e la reputazione della Società.

In particolare, i soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dalla presente Parte Speciale;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/controparti contrattuali anche stranieri;
4. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità o eversive dell'ordine democratico quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
5. non utilizzare strumenti anonimi e/o non tracciabili per il compimento di operazioni di trasferimento di importi rilevanti;
6. effettuare un costante monitoraggio dei flussi finanziari aziendali.

CAPITOLO C.4

Principi comportamentali specifici

Nello svolgimento delle Attività Sensibili individuate nella presente parte Speciale, la Società deve uniformarsi ai seguenti principi:

- nella predisposizione delle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto, la Società adotta presidi formalizzati volti a far sì che:
 - i. non vengano indicati elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti;
 - ii. non vengano indicati elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
 - iii. non venga indicata una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi;
 - iv. non vengano fatti decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle medesime così come per il successivo versamento delle imposte da esse risultanti.

La Società si impegna, altresì, a garantire l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione nelle dichiarazioni tributarie con riferimento, a titolo esemplificativo, a:

- il controllo sull'effettività delle prestazioni rispetto alle fatture emesse;
- la verifica della veridicità delle dichiarazioni rispetto alle scritture contabili;
- la verifica della corrispondenza tra i certificati eventualmente rilasciati, o comunque dovuti, in qualità di sostituto d'imposta e l'effettivo versamento delle ritenute.

È fatto, altresì, divieto di:

- i. emettere fatture o altri documenti contabili relativi ad operazioni in tutto o in parte inesistenti, a livello oggettivo o soggettivo;

- ii. emettere fatture o altri documenti contabili per corrispettivi superiori agli importi reali;
- iii. effettuare pagamenti a fronte dell'emissione di fatture relative ad attività non ricevute dal soggetto che ha emesso la fattura.

Nell'ambito dell'Attività Sensibile, inoltre, la Società:

- i. disciplina l'interazione tra tutte le figure coinvolte nella compilazione delle dichiarazioni di natura contabile (tra cui i bilanci) e fiscale, attraverso una precisa specificazione dei singoli ruoli;
- ii. assicura la custodia in modo corretto e ordinato delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali;
- iii. assicura l'attuazione di un periodico monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura contabile;
- iv. garantisce che non vengano indirizzati flussi di denaro nei confronti di soggetti che figurino nelle *blacklist* internazionali ovvero su conti intestati a soggetti diversi da quelli che hanno diritto di riceverli, ovvero ubicati in un Paese diverso da quello ove detti soggetti hanno sede;
- v. prevede nei contratti clausole standard che richiamino il rispetto dei principi comportamentali di cui al presente Modello al fine di prevenire la responsabilità della Società ex D.Lgs. 231/2001.

Nella gestione degli strumenti di pagamento diversi dal contante, la Società garantisce:

- i. una chiara identificazione dei soggetti intestatari di strumenti di pagamento diversi dal contante (ad esempio, carte di credito aziendali e carte carburante) e delle modalità di autorizzazione dei pagamenti;
- ii. l'attribuzione delle carte di credito aziendali (e degli altri strumenti di pagamento) secondo criteri di assegnazione predeterminati, nel rispetto dei passaggi autorizzativi previsti per la concessione delle stesse;
- iii. il rispetto del divieto di falsificare, alterare, utilizzare indebitamente – non essendone titolare e al fine di trarne profitto per sé o altri (compresa la Società) – carte di credito o di pagamento, ogni documento che abiliti al prelievo di denaro contante o all'acquisto di beni o servizi e ogni altro strumento di pagamento diverso dai contanti (ad esempio, è fatto divieto di utilizzare carte di

credito non riferibili alla Società per effettuare pagamenti per conto di quest'ultima e, in particolare, carte di credito intestate ad altri soggetti – persone fisiche o giuridiche – anche se collegati alla Società);

- iv. il rispetto del divieto di produrre, importare, esportare, vendere, trasportare, distribuire ovvero mettere a disposizione apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono ideati al fine di commettere delitti con strumenti di pagamento diversi dai contanti;
- v. il rispetto del divieto di alterare in qualsiasi modo il funzionamento di sistemi informatici o telematici o intervenire sui contenuti di detti sistemi o comunque utilizzare gli stessi al fine di realizzare un trasferimento di denaro, di valore monetario o di valuta virtuale.

Con riferimento agli aspetti relativi alla selezione e alla gestione dei rapporti con Consulenti, *Outsourcer* e Fornitori, si richiamano espressamente, in quanto applicabili, le regole già illustrate nella Parte Speciale A.

CAPITOLO C.5

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella policy aziendale adottata ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

CAPITOLO C.6

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, sono previsti i seguenti flussi informativi nei confronti dell'Organismo di Vigilanza:

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Legale	Informativa circa controparti contrattuali che hanno sede in Paesi non cooperativi o compresi nelle liste nominative pubblicate sul sito dell'UIF (Banca d'Italia).	Ad evento
Amministratore Unico	Indicazione dei contratti di sponsorizzazione eventualmente stipulati e delle iniziative sociali intraprese.	Annuale
CFO	Relazione su: <ul style="list-style-type: none">- eventuali pagamenti in contanti (o tramite altri strumenti anonimi) eseguiti o ricevuti per valori pari o superiori a Euro 1.000, specificando i) il soggetto destinatario e ii) il motivo del pagamento in contanti;- pagamenti rilevanti effettuati o ricevuti a favore di o da enti terzi rispetto alla Società con sede legale in paesi a rischio di terrorismo o in paradisi fiscali;- eventuali criticità in riferimento all'utilizzo di strumenti di pagamento diversi dai contanti (ad esempio, le carte di credito aziendali).	Ad evento

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

**PARTE SPECIALE – D – REATI DI OMICIDIO COLPOSO E LESIONI GRAVI
O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA
TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO**

**REATI CONTRO LA PERSONALITÀ INDIVIDUALE E IMPIEGO DI
CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE**

DEFINIZIONI:

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale “D”.

UNI ISO 45001:2018: norma internazionale per la definizione degli *standard* relativi al sistema di gestione per la salute e sicurezza sul lavoro.

Datore di Lavoro: il soggetto titolare del rapporto di lavoro con il Lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il Lavoratore presta la propria attività, ha la responsabilità, in virtù di apposita delega, dell'organizzazione stessa o del singolo settore, in quanto esercita i poteri decisionali e di spesa.

DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze: 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.

DVR o Documento di Valutazione dei Rischi: il documento redatto dal Datore di Lavoro contenente una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuali adottati a seguito di 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 ha 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 ed addestramento.

Lavoratori: persone che, indipendentemente dalla tipologia contrattuale, svolgono un'attività lavorativa nell'ambito dell'organizzazione della Società.

Medico Competente: il medico in possesso di uno dei titoli e dei requisiti formali e professionali indicati nel Testo Unico Sicurezza che collabora con il Datore di Lavoro ai fini della valutazione dei rischi e al fine di effettuare la Sorveglianza Sanitaria e adempiere tutti gli altri compiti di cui al Testo Unico Sicurezza.

RLS o Rappresentante dei Lavoratori per la Sicurezza: il soggetto eletto o designato per rappresentare i Lavoratori in relazione agli aspetti della salute e sicurezza durante il lavoro.

RSPP o Responsabile del Servizio di Prevenzione e Protezione: il soggetto in possesso delle capacità e dei requisiti professionali indicati nel Testo Unico Sicurezza, designato dal Datore di Lavoro, a cui risponde, per coordinare il Servizio di Prevenzione e Protezione.

Sorveglianza Sanitaria: 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.

SPP o Servizio di Prevenzione e Protezione: l'insieme delle persone, sistemi e mezzi esterni o interni alla Società finalizzati all'attività di prevenzione e protezione dei rischi professionali per i Lavoratori.

SSL: Salute e Sicurezza dei Lavoratori.

Testo Unico Sicurezza: Il D. Lgs. 9 aprile 2008, n. 81 di attuazione dell'articolo 1 della Legge 3 agosto 2007, n. 123 in materia di tutela della salute e della sicurezza nei luoghi di lavoro.

CAPITOLO D.1

LE FATTISPECIE DI REATO

Le fattispecie dei reati nei reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies*, D.Lgs. 231/2001)

L'art. 25 *septies* del Decreto, originariamente introdotto dalla legge 3 agosto 2007 n. 123 e successivamente sostituito nell'attuale formulazione dall'art. 300 del Testo Unico Sicurezza, prevede l'applicazione di sanzioni pecuniarie ed interdittive agli enti i cui esponenti commettano i reati di cui agli artt. 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 sulla salute e sicurezza sul lavoro.

Omicidio colposo (art. 589 c.p.)

Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto.

Lesioni personali colpose gravi o gravissime (art. 590, comma 3, c.p.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa ad altro soggetto lesioni gravi o gravissime.

Ai sensi del comma 1 dell'art. 583 c.p., 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 c.p., *“la lesione è considerata invece gravissima se dal fatto deriva:*

- una malattia certamente o probabilmente insanabile;*
- la perdita di un senso;*
- 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;*

- *la deformazione, ovvero lo sfregio permanente del viso*”.

Perché si venga a configurare la responsabilità amministrativa della Società ai sensi del Decreto, l'art. 5 dello stesso esige che i reati siano stati commessi nel suo interesse o a suo vantaggio (ad esempio – secondo l'interpretazione giurisprudenziale –, in termini di risparmi di costi o di tempi).

Le fattispecie di Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello stato e favoreggiamento dell'immigrazione clandestina (art. 25-*duodecies* D.Lgs. 231/2001)

L'art. 25-*duodecies* del Decreto richiama al primo comma il reato di Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 e 12-bis, D.Lgs. 286/1998).

Tale ipotesi di reato si configura nei confronti del datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo o sia stato revocato o annullato.

L'art. 22, comma 12-bis del D.Lgs. 286/1998 prevede un aumento delle pene da un terzo alla metà per i datori di lavoro che:

- occupano irregolarmente più di tre lavoratori irregolari;
- occupano minori in età non lavorativa;
- sfruttano lavoratori di cui all'art. 603 *bis* del codice penale (vale a dire, oltre alle ipotesi sopra citate, se i lavoratori sono esposti a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro).

La responsabilità dell'ente è configurabile soltanto quando il reato in questione sia aggravato dal numero dei soggetti occupati o dalla minore età degli stessi o, infine, dalla prestazione del lavoro in condizioni di pericolo grave.

L'art. 25 *duodecies* è stato oggetto di modifiche ad opera della Legge 161 del 4 novembre 2017 che ha introdotto il richiamo all'art. 12 (“Disposizioni contro le immigrazioni clandestine”), D.Lgs. 25 luglio 1998, n. 286, limitatamente ai commi di seguito riportati.

Art. 12, commi 3, 3 bis, 3 ter, D.Lgs. 286/1998

“3. Salvo che il fatto costituisca più grave reato, è punito chiunque, in violazione delle disposizioni del D.Lgs. 286/1998 promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, per ogni persona nel caso in cui:

- a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;*
- b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;*
- c) la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;*
- d) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;*
- e) gli autori del fatto hanno la disponibilità di armi o materie esplosive.*

3-bis. *Se i fatti di cui al comma 3 sono commessi ricorrendo due o più delle ipotesi di cui alle lettere a), b), c), d) ed e) del medesimo comma, la pena ivi prevista è aumentata.*

3-ter. *La pena detentiva è aumentata se i fatti di cui ai commi 1 e 3:*

- a) sono commessi al fine di reclutare persone da destinare alla prostituzione o comunque allo sfruttamento sessuale o lavorativo ovvero riguardano l'ingresso di minori da impiegare in attività illecite al fine di favorirne lo sfruttamento;*
- b) sono commessi al fine di trarre profitto, anche indiretto”.*

Articolo 12, comma 5, D.Lgs. 286/1998

“Fuori dei casi previsti dai commi precedenti, e salvo che il fatto non costituisca più grave reato, la norma punisce chiunque, al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero o nell'ambito delle attività punite a norma del presente articolo, favorisce la permanenza di questi nel territorio dello Stato in violazione delle disposizioni di cui al D.Lgs. 286/1998.

Quando il fatto è commesso in concorso da due o più persone, ovvero riguarda la permanenza di cinque o più persone, è previsto un aumento di pena da un terzo alla metà”.

Le fattispecie dei delitti contro la personalità individuale (art. 25-quinquies, D.Lgs. n. 231/2001)

Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)

La norma punisce chiunque (i) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori ovvero, (ii) utilizza, assume o impiega manodopera anche mediante l'attività di intermediazione di cui al punto (i), sottoponendo i lavoratori a condizioni di sfruttamento e approfittando del loro stato di bisogno.

Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni: 1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato; 2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; 3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro; 4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà: 1) il fatto che il numero di lavoratori reclutati sia superiore a tre; 2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa; 3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

CAPITOLO D.2

Con riguardo ai Reati considerati nella presente Parte Speciale, la Società ha individuato le seguenti Attività Sensibili:

1. adempimento degli obblighi normativi in materia di salute e sicurezza nei luoghi di lavoro;
2. assunzione del personale;
3. selezione degli appaltatori e subappaltatori.

CAPITOLO D.3

REGOLE GENERALI

D.3.1 Principi generali di comportamento

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori così come individuati dall'art. 15 Testo Unico Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del medesimo decreto si prevede quanto segue.

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

- a) organigramma aziendale;
- b) CCNL;
- c) documenti di Valutazione dei Rischi con i relativi documenti integrativi;
- d) ogni procedura operativa o organizzativa in materia di salute e sicurezza sul lavoro (incluse quelle per la gestione e prevenzione del rischio contagio Covid-19).

D.3.2 Compiti e responsabilità

Nella definizione dei compiti organizzativi ed operativi, devono essere esplicitati e resi noti anche quelli relativi alle attività di sicurezza di rispettiva competenza, nonché le responsabilità connesse all'esercizio delle stesse ed i compiti di ispezione, verifica e sorveglianza in materia di Sicurezza sul Lavoro.

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.

Il Datore di Lavoro

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

- 1) valutare tutti i rischi per la sicurezza e per la salute dei lavoratori;
- 2) elaborare, all'esito di tale valutazione, i Documenti di Valutazione dei Rischi contenente tra l'altro:

- una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante

il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa;

- l'indicazione delle eventuali misure di prevenzione e di protezione attuate e degli eventuali dispositivi di protezione individuale adottati a seguito della suddetta valutazione dei rischi (artt. 74–79 Testo Unico Sicurezza);
- 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 dei nominativi di RSPP, RLS e Medico Competente che abbiano partecipato alla valutazione del rischio.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con l'RSPP e il Medico Competente. La valutazione dei rischi è oggetto di consultazione preventiva con il Rappresentante dei Lavoratori per la Sicurezza.

3) designare i Responsabili del Servizio di Prevenzione.

Al Datore di Lavoro sono attribuiti numerosi altri compiti dallo stesso delegabili a soggetti qualificati. Tali compiti, previsti dal Testo Unico Sicurezza, riguardano, tra l'altro: a) la nomina del Medico Competente per l'effettuazione della Sorveglianza Sanitaria; b) la preventiva designazione dei 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; c) l'adempimento degli obblighi di informazione, formazione ed addestramento; d) la convocazione della riunione periodica di cui all'art. 35 Testo Unico Sicurezza; e) l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza del lavoro, ecc..

In relazione a tali compiti ed a ogni altro dovere incombente sul Datore di Lavoro che possa essere da questi delegato ai sensi del Testo Unico Sicurezza, la suddetta delega 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.

I Dirigenti possono a loro volta, previa intesa con il Datore di Lavoro delegante, sub-delegare specifiche funzioni in materia di salute e sicurezza sul lavoro alle medesime condizioni di cui sopra. Siffatta sub-delega di funzioni non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale sia conferita tale sub-delega non può, a sua volta, delegare le funzioni delegate.

Il Datore di Lavoro provvede, inoltre, alla formalizzazione della nomina dei preposti attraverso un atto che preveda la tracciabilità della formale accettazione dell'incarico da parte di quest'ultimi.

Il Datore di Lavoro fornisce al Servizio di Prevenzione e Protezione ed ai Medici Competenti informazioni in merito a:

- a) la natura dei rischi;
- b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
- c) la descrizione dei luoghi di lavoro e degli eventuali processi produttivi;
- d) i dati relativi agli infortuni e quelli relativi alle malattie professionali.

Il Servizio di Prevenzione e Protezione (SPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro si avvale, eventualmente anche ricorrendo a soggetti esterni alla Società, del Servizio di Prevenzione e Protezione dei rischi professionali, che provvede:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- ad elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e i sistemi di controllo di tali misure;
- ad elaborare le procedure di sicurezza per le varie attività aziendali;

- a proporre i programmi di informazione e formazione dei Lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35 Testo Unico Sicurezza;
- a fornire ai Lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria.

Qualora, nell'espletamento dei relativi compiti, il RSPP della Società verificasse la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro, questi dovrà darne immediata comunicazione anche all'OdV.

L'eventuale sostituzione del RSPP dovrà altresì essere comunicata all'OdV con l'espressa indicazione delle motivazioni a supporto di tale decisione.

Il RSPP deve avere capacità e requisiti professionali in materia di prevenzione e sicurezza e, precisamente deve:

- essere in possesso di un titolo di istruzione secondaria superiore;
- aver partecipato a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro;
- aver conseguito attestato di frequenza di specifici corsi di formazione in materia di prevenzione e protezione dei rischi;
- aver frequentato corsi di aggiornamento.

Il RSPP è coinvolto ed invitato alle riunioni dell'OdV relativamente alle materie di competenza.

Il Medico Competente

Il Medico Competente provvede tra l'altro 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 e custodire, 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 SPP, redigendo specifico verbale, con la frequenza prestabilita in relazione alle caratteristiche dell'Unità produttiva 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 Testo Unico 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.

Il Medico Competente deve essere in possesso di uno dei titoli *ex art.* 38, D.Lgs. n. 81/2008 e, precisamente:

- di specializzazione 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 ed altre specializzazioni individuate, ove necessario, con decreto del Ministro della Sanità di concerto con il Ministro dell'Università e della Ricerca Scientifica e Tecnologica; oppure
- essere docente o libero docente 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;
- essere in possesso dell'autorizzazione di cui all'art. 55, D.Lgs. n. 277/91, che prevede una comprovata esperienza professionale di almeno 4 anni.

Il Rappresentante dei Lavoratori per la Sicurezza (RLS)

È il soggetto eletto o designato, 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.

Riceve, a cura del Datore di Lavoro o di un suo delegato, la prevista formazione specifica in materia di salute e sicurezza.

Il RLS:

- accede ai luoghi di lavoro;
- è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- è consultato sulla designazione del RSPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso e del Medico Competente;
- è consultato in merito all'organizzazione delle attività formative;
- promuove l'elaborazione, l'individuazione e l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori;
- partecipa alla "riunione periodica di prevenzione e protezione dai rischi";
- riceve informazioni inerenti la valutazione dei rischi e le misure di prevenzione relative e, ove ne faccia richiesta e per l'espletamento della sua funzione, copia del Documento di Valutazione dei Rischi e del DUVRI.

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

Il Committente

Il Committente, tra l'altro:

- si attiene ai principi e alle misure generali di tutela di cui all'art. 15 del Testo Unico Sicurezza;
- verifica l'idoneità tecnico-professionale delle imprese affidatarie, delle imprese esecutrici e dei Lavoratori autonomi in relazione ai lavori da affidare, anche attraverso l'iscrizione alla Camera di commercio, industria e artigianato e del documento unico

di regolarità contributiva corredato da autocertificazione in ordine al possesso dei requisiti di cui all'allegato XVII del Testo Unico Sicurezza.

Il Responsabile dei Lavori

E' il soggetto che può essere incaricato – in relazione all'organizzazione – dal Committente di svolgere i compiti ad esso attribuiti dal Testo Unico Sicurezza. In particolare, ad esso, se nominato, competono, per la parte delegata, gli obblighi che il Titolo IV del Testo Unico Sicurezza pone in capo al Committente.

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 in particolare:

- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro o dal suo delegato ai fini della protezione collettiva ed individuale;
- utilizzare correttamente le apparecchiature da lavoro nonché gli eventuali dispositivi di sicurezza;
- segnalare immediatamente al Datore di Lavoro 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 RLS;
- non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al Datore di Lavoro o al suo delegato 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.

I lavoratori di aziende che svolgono per la Società attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

E.3.3 Informazione, formazione e addestramento

Informazione

L'informazione che la Società riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

- a) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate dalla Società in tema di SSL;
- b) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di SSL adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale.

Ciò premesso, la Società, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun Dipendente, è tenuta ai seguenti oneri informativi:

- la Società deve fornire adeguata informazione ai dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) circa i rischi specifici dell'impresa, per quanto limitati, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- deve essere data evidenza dell'informativa erogata per la gestione del pronto soccorso, emergenza, evacuazione e prevenzione incendi e devono essere verbalizzati gli eventuali incontri;
- i dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) devono ricevere informazione sulla nomina del RSPP, sul Medico Competente e sugli addetti ai compiti specifici per il pronto soccorso, salvataggio, evacuazione e prevenzione incendi;
- deve essere formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Lavoratori;
- il RSPP e/o il Medico Competente devono essere coinvolti nella definizione delle informazioni;
- la Società deve organizzare periodici incontri tra le funzioni preposte alla sicurezza sul lavoro;

- la Società deve coinvolgere il Rappresentante dei Lavoratori per la Sicurezza nella organizzazione della attività di rilevazione e valutazione dei rischi, nella designazione degli addetti alla attività di prevenzione incendi, pronto soccorso ed evacuazione;
- la Società deve strutturare e garantire l'efficace funzionamento di uno strumento che consenta il costante e puntuale monitoraggio sulle fonti normative e tecniche emesse da enti e autorità preposte relativamente alla gestione del rischio contagio da Covid-19;
- la Società deve attivare un meccanismo di studio e valutazione delle singole misure anti contagio da Covid-19 emesse dalle Autorità, al fine di garantirne la piena e rigorosa applicazione secondo le caratteristiche specifiche della realtà di impresa.

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 Società, in considerazione dei diversi ruoli, responsabilità, capacità e dei rischi cui è esposto ciascun Lavoratore, fornisce tra l'altro, adeguata informazione ai Lavoratori sulle seguenti tematiche:

- sui rischi per la salute e sicurezza sul lavoro, connessi all'attività dell'impresa 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 pericoli connessi all'uso di sostanze e preparati pericolosi;
- sui nominativi dei Lavoratori incaricati delle misure di emergenza e di primo soccorso, nonché del RSPP e del Medico Competente;
- sulla normativa (leggi, regolamenti, protocolli condivisi e linee guida di categoria) e misure di contenimento del contagio da Covid-19.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione.

Formazione e addestramento

La Società 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, ove presente, debbono partecipare alla stesura del piano di formazione, approvato annualmente dal Datore di Lavoro;
- il suddetto piano di formazione potrà essere implementato, per temi specifici, su segnalazione dei RLS o sulla base di proposte provenienti dai responsabili territoriali;
- ulteriori attività integrative a tale piano dovranno essere attuate in presenza di innovazioni tecnologiche, nuove attrezzature o necessità di introdurre nuove procedure di lavoro;
- 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:
 - a) uso delle attrezzature di lavoro;
 - b) uso dei dispositivi di protezione individuale;
 - c) movimentazione manuale carichi;
 - d) uso dei videoterminali;
 - e) segnaletica visuale, gestuale, vocale, luminosa e sonora;
- gli addetti a specifici compiti in materia di emergenza devono ricevere specifica formazione;

- i Dirigenti e i preposti ricevono a cura del Datore di Lavoro, un'adeguata e specifica formazione e un aggiornamento periodico in relazione ai propri compiti in materia di SSL; i contenuti di tale formazione comprendono:
 - a) principali soggetti coinvolti e i relativi obblighi;
 - b) definizione e individuazione dei fattori di rischio;
 - c) valutazione dei rischi;
 - d) individuazione delle misure tecniche, organizzative e procedurali di prevenzione e protezione.
- il Datore di Lavoro riceve un'adeguata e specifica formazione e un aggiornamento periodico in relazione ai propri compiti in materia di SSL;
- la Società 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 non possono essere adibiti in autonomia ad attività operativa ritenuta più a rischio infortuni se non dopo l'accertamento del possesso 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, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente.

E.3.4 Flussi informativi e cooperazione

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Società si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori.

A tal proposito la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

a) dal basso verso l'alto

Ciascuno dei Lavoratori ha la possibilità di portare agevolmente a conoscenza del proprio superiore gerarchico osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale;

b) dall'alto verso il basso

La Società garantisce ai Destinatari un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- eventuali nuovi rischi in materia di salute e sicurezza dei Lavoratori;
- modifiche nella struttura organizzativa adottata dalla Società per la gestione della salute e sicurezza dei Lavoratori;
- contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- ogni altro aspetto inerente alla salute e alla sicurezza dei Lavoratori.

Documentazione aziendale

La Società provvede alla conservazione, sia su supporto cartaceo che informatico, dei documenti rilevanti in relazione alla sicurezza sul luogo di lavoro. Ad esempio, vengono così conservati le cartelle sanitarie e il Documento di Valutazione dei Rischi.

La Società è altresì chiamata a garantire che:

- il RSPP, ogni Medico Competente e gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente;
- venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente;
- venga mantenuto aggiornato il registro degli infortuni, riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;
- vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature ed eventuali dispositivi di protezione individuale forniti dai costruttori;

- venga conservata ogni procedura adottata dalla Società per la gestione della salute e sicurezza sui luoghi di lavoro;
- tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'OdV;
- nell'ipotesi di esposizione ad agenti cancerogeni o mutageni e biologici sia predisposto il registro degli esposti;
- siano conservati i documenti che registrano gli adempimenti espletati in materia di sicurezza e igiene sul lavoro;
- avvenga la nomina formale del Responsabile del Servizio di Prevenzione e Protezione (RSPP), del Medico Competente, degli incaricati dell'attuazione delle misure di emergenza e primo soccorso, nonché degli eventuali Dirigenti e Preposti;

D.3.5 L'attività di monitoraggio

La Società deve assicurare un costante ed efficace monitoraggio delle misure di prevenzione e protezione adottate sui luoghi di lavoro.

A tale scopo la Società:

- assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- assicura un costante monitoraggio dell'adeguatezza e della funzionalità di tali misure a raggiungere gli obiettivi prefissati e della loro corretta applicazione;
- compie approfondite analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema e di identificare le eventuali azioni correttive da intraprendere.

L'attività di monitoraggio viene assicurata attraverso il rispetto delle norme interne che prevedono:

- i ruoli ed i compiti dei soggetti responsabili delle seguenti attività dell'emissione di procedure ed istruzioni in materia di salute e sicurezza sui luoghi di lavoro;
- l'acquisizione da parte dell'Organismo di Vigilanza, in qualunque momento e senza necessità di autorizzazione, di tutta la documentazione aziendale relativa ai controlli sulle procedure e le istruzioni di sicurezza;

- il controllo sullo svolgimento dei piani aziendali di informazione e formazione;
- l’emanazione delle istruzioni relative all’utilizzo delle attrezzature munite di videoterminali;
- la tempistica e la comunicazione dei risultati riscontrati;
- il sistema sanzionatorio applicato in caso di violazione delle misure in materia di salute e sicurezza sui luoghi di lavoro.

Al fine di adempiere adeguatamente all’attività di monitoraggio ora descritta, la Società, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione.

La Società garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.

CAPITOLO D.4

I CONTRATTI DI APPALTO E LE ASSUNZIONI DI CITTADINI EXTRA UE

La Società deve predisporre e mantenere aggiornato l'elenco delle imprese che operano sulla base di un contratto d'appalto all'interno dei propri uffici.

Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espliciti riferimenti agli adempimenti di cui all'art. 26, Testo Unico Sicurezza, tra questi, in capo al Datore di Lavoro:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso l'acquisizione
 - del certificato di iscrizione alla camera di commercio, industria e artigianato;
 - dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'art. 4, D.P.R. 28 dicembre 2000, n. 445;
 - dell'elenco del personale dipendente che potrà avere accesso ai locali e alle aree di pertinenza della Società, con espressa indicazione del personale dell'appaltatore che svolge la funzione di preposto;
 - di dichiarazione attestante la formazione ricevuta dai lavoratori per i quali si richiede l'accesso;
 - di copie delle specifiche autorizzazioni rilasciate da enti pubblici e/o privati (se necessarie in relazione all'adempimento dell'attività);
 - di dichiarazione con cui si attesti di non essere oggetto di provvedimenti di sospensione o interdittivi di cui all'art. 14 del D.Lgs. 81/08;
 - di copia del Libro Unico del Lavoro nella parte relativa ai dipendenti coinvolti;
 - di eventuale copia di polizza assicurativa;
- fornire informazioni dettagliate agli appaltatori circa gli eventuali 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 per ogni appalto che rientri nel perimetro di applicazione dell'art. 26 Testo Unico Sicurezza, un Documento di Valutazione di Rischi 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.

Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro. A tali dati può accedere, su richiesta, il Rappresentante per la Sicurezza dei Lavoratori.

Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

L'imprenditore committente risponde in solido con l'appaltatore, nonché con ciascuno degli eventuali ulteriori subappaltatori, per tutti i danni per i quali il lavoratore, dipendente dall'appaltatore o dal subappaltatore, non risulti indennizzato ad opera dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro.

La Società, infine:

- a. considera sempre prevalente la tutela dei diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione economica;
- b. vieta l'assunzione di dipendenti stranieri privi di permesso di soggiorno regolare e vieta di conferire incarichi ad appaltatori e/o subappaltatori che, al contrario, se ne avvalgano;
- c. assicura massima tracciabilità e trasparenza nella gestione dei rapporti con società che svolgono attività in appalto per conto della Società.

Con riguardo all'instaurazione di rapporti di lavoro, la Società:

- in caso di un'eventuale assunzione di cittadini stranieri residenti in Paesi Extracomunitari, si attiva presso le Autorità competenti al fine di ottenere tutta la documentazione necessaria a consentire l'ingresso legale in Italia del cittadino straniero e l'instaurazione di un rapporto di lavoro regolare;
- in caso di un'eventuale assunzione di cittadini stranieri già soggiornanti in Italia, verifica che i medesimi siano in possesso di un permesso di soggiorno regolare o che

in caso di scadenza dello stesso i medesimi abbiano provveduto ad avviare le pratiche per il rinnovo;

- controlla che, in occasione della scadenza dei permessi di soggiorno di eventuali dipendenti stranieri, questi ultimi abbiano provveduto ad avviare le relative pratiche di rinnovo, assicurando loro collaborazione nel rilascio della documentazione attestante l'impiego regolare presso la Società;
- assicura che, qualora l'adempimento delle attività descritte ai punti precedenti avvenisse eventualmente ricorrendo ai servizi di un'agenzia esterna specializzata, il rapporto con quest'ultima sia disciplinato da accordo scritto, il quale preveda – *inter alia* – l'obbligo dell'agenzia esterna a non porre in essere comportamenti che violino le disposizioni di cui al Decreto 231 e a rispettare per quanto applicabile il Modello 231 della Società.

Con riguardo all'affidamento in appalto di servizi, la Società adotta presidi idonei a garantire che l'appaltatore e/o il subappaltatore non impieghino cittadini stranieri privi di permesso di soggiorno o con permesso di soggiorno irregolare. A tal fine la Società si assicura che nei contratti di appalto siano inseriti i seguenti presidi:

- la garanzia da parte dell'appaltatore di impiegare nella prestazione di servizi a favore della Società esclusivamente lavoratori stranieri lecitamente soggiornanti in Italia e con rapporto di lavoro regolare;
- l'obbligo, contrattualmente previsto, a carico dell'appaltatore/subappaltatore di rispettare a sua volta la normativa in materia di lavoro;
- l'impegno da parte dell'appaltatore di comunicare l'elenco, con specificazione delle generalità, dei dipendenti preposti allo svolgimento del servizio in appalto e subappalto presso la Società e a comunicare con un congruo preavviso ogni eventuale variazione dell'elenco medesimo;
- l'impegno da parte dell'appaltatore a fornire all'atto della sottoscrizione del contratto e, successivamente, con periodicità stabilita dalle parti, copia del Documento Unico di Regolarità Contributiva relativo alla posizione amministrativa dell'appaltatore e dei propri subappaltatori rilasciato dalle autorità competenti;
- la facoltà da parte della Società di richiedere in ogni momento copia del Libro Unico

del Lavoro tenuto dall'appaltatore e dagli eventuali subappaltatori;

- l'obbligo dell'appaltatore a non porre in essere comportamenti che violino le disposizioni di cui al Decreto 231 e a rispettare per quanto applicabile il Modello 231 della Società.

La Società, inoltre, si assicura che:

- i lavoratori operanti alle dipendenze o, comunque, al servizio degli appaltatori e/o subappaltatori non operino in condizioni di sfruttamento;

con specifico riferimento ai rapporti con i Fornitori, la Società prevede contrattualmente – in aggiunta a quanto previsto al punto precedente – l'obbligo a carico degli stessi di rispettare la normativa in materia di lavoro, con particolare attenzione al lavoro minorile ed a quanto disposto dalla legge in tema di salute e sicurezza.

CAPITOLO D.5

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella policy aziendale adottata ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- esaminare la documentazione e le motivazioni della scelta del management in merito alle linee produttive ritenute necessarie per la produzione e dunque da mantenere aperte, nonché agli uffici da organizzare secondo la modalità *smartworking*;

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

CAPITOLO D. 6

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, sono previsti i seguenti flussi informativi nei confronti dell'Organismo di Vigilanza:

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Responsabile della Sicurezza	Infortuni sul luogo di lavoro.	Ad evento
Amministrazione del personale	Eventuali sanzioni disciplinari nei confronti dei dipendenti per violazione delle norme sulla sicurezza.	Ad evento
	Informativa circa l'assunzione di dipendenti residenti in paesi extra UE.	

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

PARTE SPECIALE – E – REATI AMBIENTALI

CAPITOLO E. 1

LE FATTISPECIE DI REATO

Si provvede qui di seguito a fornire un elenco dei reati contemplati nella presente Parte Speciale, così come indicati all'art. 25 *undecies* del Decreto (di seguito i "Reati Ambientali").

E.1.1 Fattispecie di cui al Codice Penale

- Inquinamento ambientale (art. 452 *bis* c.p.);
- Disastro ambientale (art. 452 *quater* c.p.);
- Delitti colposi contro l'ambiente (art. 452 *quinqüies* c.p.);
- Traffico e abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.);
- Associazione a delinquere con aggravante ambientale (art. 452 *octies* c.p.);
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 *bis* c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 *bis* c.p.);
- Attività organizzate per il traffico illecito di rifiuti (art. 452 *quaterdecies*).

E.1.2 Fattispecie di cui al D. Lgs. 152/2006 (Codice dell'Ambiente)

- l'effettuazione di scarichi di acque reflue industriali contenenti sostanze pericolose (art. 137);
- la raccolta, trasporto, smaltimento, commercio di rifiuti in mancanza di autorizzazione (art. 256);
- l'inquinamento del suolo, sottosuolo, acque superficiali o sotterranee con il superamento delle concentrazioni soglia (art. 257);
- la violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258);
- il traffico illecito dei rifiuti (art. 259);

- la falsa indicazione delle caratteristiche dei rifiuti nei certificati e l'utilizzo degli stessi (art. 260 *bis*);
- il superamento dei valori limite di emissione (art. 279).

E.1.3 Fattispecie di cui alla Legge n. 150/1992

- l'importazione o l'esportazione senza licenza, l'utilizzo difforme, il trasporto, il commercio o la detenzione degli esemplari elencati nel Regolamento CE 338/97;
- la detenzione di mammiferi e rettili selvatici o in cattività;
- la falsificazione o l'alterazione di documenti per ottenere licenze o certificati.

E.1.4 Fattispecie di cui alla Legge n. 549/1993

In tema di tutela dell'ozono stratosferico (L. 549/1993), sono invece punite la produzione, il consumo, l'importazione, l'esportazione, la commercializzazione e la detenzione delle sostanze lesive secondo quanto previsto dal Regolamento CE n. 3093/94 (quest'ultimo abrogato e sostituito da ultimo dal Regolamento CE n. 1005/2009).

E.1.5 Fattispecie di cui al D. Lgs. n. 202/2007

Infine, sono richiamati anche i reati relativi all'inquinamento provocato dalle navi e in particolare il versamento colposo o doloso in mare di sostanze nocive (artt. 8 e 9 D. Lgs. 202/2007).

CAPITOLO E.2

Qui di seguito è indicata l'Attività Sensibile identificata con riferimento ai reati ambientali:

1. selezione e gestione dei rapporti con fornitori di prestazioni di gestione, trasporto e smaltimento dei rifiuti (compreso lo smaltimento di apparecchiature d'ufficio).

CAPITOLO E.3

E.3.1 Principi di comportamento

La politica dell'impresa in materia di contenimento dei rischi di commissione dei Reati Ambientali si ispira ai seguenti principi:

Nell'ambito delle proprie attività, la gestione dei rifiuti – sia per i rifiuti pericolosi sia per quelli non pericolosi – è affidata a fornitori esterni, in relazione ai quali la Società svolge un'attività di monitoraggio nel rispetto delle prescrizioni normative vigenti.

A tal fine, la Società:

- a) definisce i principali adempimenti da adottare in ambito aziendale in merito alla gestione delle diverse tipologie di rifiuti prodotti dalla Società (soprattutto in riferimento alla gestione di rifiuti speciali, quali toner e materiale elettronico e informatico);
- b) provvede alla raccolta e alla classificazione dei rifiuti prodotti nell'ambito delle attività aziendali in conformità a quanto stabilito dalle disposizioni normative vigenti;
- c) informa adeguatamente il personale dipendente in merito alla differenziazione e raccolta di rifiuti, soprattutto in relazione alla separazione e al deposito dei rifiuti speciali in appositi contenitori e/o in luoghi specificamente dedicati;
- d) affida le attività di gestione, trasporto, recupero e smaltimento dei rifiuti esclusivamente a imprese autorizzate e nel rispetto delle procedure aziendali relative alla selezione dei fornitori di servizi in *outsourcing*;
- e) nei contratti con i fornitori dei servizi di gestione, trasporto, recupero e smaltimento di rifiuti speciali prevede apposite clausole che consentono alla Società stessa di risolvere, con effetto immediato, il contratto medesimo nel caso in cui dovessero essere riscontrate irregolarità, da parte dei fornitori e dei propri subfornitori, nella gestione dei rifiuti prodotti dalla Società medesima;
- f) detiene un registro nel quale sono archiviate le informazioni riguardanti gli appaltatori e/o subappaltatori ai quali vengono affidate le attività di raccolta e smaltimento dei rifiuti, con evidenza del possesso da parte di questi delle autorizzazioni necessarie per lo svolgimento di tali attività (ad esempio, iscrizione all'Albo nazionale gestori ambientali dal quale risultino la tipologia di rifiuti, la categoria e la classe di iscrizione; autorizzazione all'esercizio dell'attività di gestione dei rifiuti rilasciata dalla competente Autorità amministrativa).

In relazione agli aspetti relativi alla selezione e alla gestione dei rapporti con Consulenti, *Outsourcer* e Fornitori si richiamano espressamente, in quanto applicabili, le regole già illustrate nella Parte Speciale A.

CAPITOLO E.4

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella *policy* aziendale adottata ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

CAPITOLO E.5

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Responsabile della Sicurezza	Eventuali criticità emerse nei rapporti con gli appaltatori incaricati della gestione, del trasporto e dello smaltimento di rifiuti.	Ad evento
Responsabile della Sicurezza	Segnalazioni ricevute in merito a tematiche ambientali (es. segnalazioni di presunte violazioni, ecc.) ovvero di criticità emerse: relazione sui fatti direttamente o indirettamente riconducibili a fattispecie di Reati ambientali.	Ad evento

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

PARTE SPECIALE – F – REATI DI CRIMINALITÀ ORGANIZZATA

CAPITOLO F.1

Le fattispecie dei reati di criminalità organizzata

La presente Parte Speciale si riferisce ai delitti di criminalità organizzata introdotti nel *corpus* del Decreto 231 all'art. 24 *ter*.

La tipologia dei reati in esame comprende le seguenti fattispecie criminose:

- “*associazione per delinquere*” di cui all'art 416 c.p.;
- “*associazione per delinquere finalizzata alla riduzione o mantenimento in schiavitù o in servitù (ex art. 600 c.p.) alla tratta di persone (ex art. 601 c.p.) o all'acquisto e alienazione di schiavi (ex art. 602 c.p.)*” di cui all'art. 416 comma 6 c.p.;
- “*associazione di stampo mafioso anche straniera*” di cui all'art. 416 *bis* c.p.;
- “*scambio elettorale politico–mafioso*” di cui all'art. 416 *ter* c.p.;
- “*sequestro di persona a scopo di rapina o di estorsione*” di cui all'art. 630 c.p.;
- “*associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope*” di cui all'art. 74 del D.P.R. n. 309/1990;
- “*delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra, di esplosivi e di armi clandestine*” di cui all'art. 407 comma 2, lett. *a*), n. 5, c.p..

Si fornisce qui di seguito una breve descrizione della fattispecie di cui all'art. 24 *ter* del Decreto ritenuta rilevante in astratto per la Società.

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

La condotta sanzionata dall'art. 416 c.p. è integrata mediante la costituzione e la conservazione di un vincolo associativo continuativo con fine criminoso **tra tre o più persone**, allo scopo di commettere una serie indeterminata di delitti, con la predisposizione di mezzi necessari per la realizzazione del programma criminoso e con la permanente consapevolezza di ciascun associato di far parte di un sodalizio e di essere disponibile ad operare per l'attuazione del programma delinquenziale.

Il reato associativo è caratterizzato, pertanto, dai seguenti elementi fondamentali:

- stabilità e permanenza: il vincolo associativo deve essere tendenzialmente stabile e destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;

- indeterminatezza del programma criminoso: l'associazione a delinquere non si configura se i partecipanti si associano al fine di compiere un solo reato; lo scopo dell'associazione deve essere quello di commettere più delitti, anche della stessa specie (in tal caso l'indeterminatezza del programma criminoso ha riguardo solo all'entità numerica);
- esistenza di una struttura organizzativa: l'associazione deve prevedere un'organizzazione di mezzi e di persone (che possono essere sia interne sia esterne alla Società) che, seppure in forma rudimentale, siano adeguati a realizzare il programma criminoso e a mettere in pericolo l'ordine pubblico.

In particolare, sono puniti coloro che promuovono, costituiscono o organizzano l'associazione, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica, definiti dal testo legislativo come "capi".

Sono puniti altresì con una pena inferiore tutti coloro che partecipano all'associazione.

Il reato in questione assume rilevanza ai fini della responsabilità amministrativa degli enti anche se commesso a livello "*transnazionale*" ai sensi dell'art. 10 della Legge 16 marzo 2006, n. 146 (legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

CAPITOLO F.2

Attività Sensibili

Le principali Attività Sensibili nell'ambito dei reati di criminalità organizzata che la Società ha individuato al proprio interno sono le seguenti:

1. selezione dei Consulenti, degli *Outsourcer*, dei Fornitori e, in generale, delle controparti contrattuali;
2. selezione e assunzione del personale.

CAPITOLO F.3

REGOLE DI COMPORTAMENTO

F.3.1 Principi generali di comportamento

La presente Parte Speciale prevede l'espreso divieto di:

- procedere all'assunzione di personale dipendente senza aver prima constatato la sussistenza di requisiti di onorabilità e affidabilità;
- instaurare rapporti con soggetti terzi – persone fisiche o giuridiche, italiane o straniere – senza aver rispettato criteri e metodologie di selezione previsti dalle procedure aziendali o dal presente Modello che consentano di accertarne onorabilità e affidabilità.

Devono altresì essere rispettati i seguenti obblighi:

- il processo di selezione delle controparti contrattuali è costantemente regolato dal principio della segregazione dei ruoli;
- la persistenza in capo a controparti contrattuali dei requisiti richiesti in fase di selezione è sottoposta a periodici controlli.

F.3.2 Principi specifici di comportamento

Nello svolgimento delle Attività Sensibili valgono i seguenti principi:

- nella selezione e successiva gestione del rapporto con controparti contrattuali (ad esempio i Consulenti) la Società garantisce che il processo di selezione avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità; a tal fine si richiama il rispetto dei principi specifici previsti nelle Parti Speciali relative ai Reati nei rapporti con la Pubblica Amministrazione, ai Reati di Corruzione tra privati e ai Reati di Riciclaggio.

In relazione agli aspetti relativi alla selezione del personale nonché alla gestione dei rapporti con Consulenti, *Outsourcer* e Fornitori, si richiamano espressamente, in quanto applicabili, le regole già illustrate nella Parte Speciale A.

CAPITOLO F.4

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nelle procedure adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

PARTE SPECIALE – G – REATI INFORMATICI
DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE

CAPITOLO G.1

LE FATTISPECIE DI REATO

Le fattispecie dei reati informatici e dei delitti in violazione del diritto d'autore

La presente Parte Speciale si riferisce ai Reati Informatici e ai Delitti in Violazione del Diritto d'Autore introdotti nel *corpus* del Decreto 231 rispettivamente all'art. 24 *bis* e all'art. 25 *nonies*.

A tal riguardo si sottolinea che, nonostante le due tipologie di reato tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Parte Speciale in quanto:

- entrambe le fattispecie di reato presuppongono, tra l'altro, un corretto utilizzo delle risorse informatiche;
- le attività sensibili potenzialmente interessate dalle due tipologie di reato in commento risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi specifici di comportamento mirano, in entrambi i casi, a garantire tra l'altro la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

Falsità in documenti informatici (art. 491 bis c.p.)

L'art. in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali in atti pubblici 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 al fine di alterare un documento pubblico.

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

Tale reato si realizza quando un soggetto “*abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo*”.

È prevista una pena più severa nei seguenti casi:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

È prevista una pena ancor più severa qualora il delitto in oggetto riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'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, detiene, produce, riproduce, diffonde, importa, comunica, consegna o mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o altri strumenti, 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*”.

La pena è più severa se il danno è commesso:

1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2. da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615 *quater* c.p., 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*).

Il delitto è integrato 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.

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 della Società 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 della Società oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

Tale reato si realizza qualora qualcuno, “allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici”.

Questo delitto è integrato, ad esempio, nel caso in cui il soggetto si procuri un virus, idoneo a danneggiare un sistema informatico o qualora si detengano, producano o si utilizzino delle *smart card* che consentono il danneggiamento di apparecchiature o di dispositivi elettronici.

Questi fatti sono punibili solo nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento. Ciò si verifica, ad esempio, qualora un dipendente introduca un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico di un concorrente.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)¹

Tale ipotesi di reato si integra qualora un soggetto fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico.

È prevista una pena più severa:

¹La Legge n. 238/2021 ha previsto un inasprimento delle pene previste per il reato di cui all'art. 617 quater c.p.

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La frodolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato è integrato, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

Questa fattispecie di reato si realizza quando qualcuno, *“fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica,*

consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi?

La condotta vietata dall'art. 617 *quinquies* è, pertanto, costituita dalla detenzione, diffusione e installazione delle apparecchiature e degli altri mezzi idonei a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, a prescindere dalla circostanza che le stesse siano o meno utilizzate. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche.

Anche la semplice detenzione di apparecchiature o altri mezzi idonei all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata, detenuta o diffusa abbia, obiettivamente, una potenzialità lesiva.

Qualora all'installazione, alla detenzione o alla diffusione, faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

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

Tale fattispecie reato si realizza quando un soggetto “distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui”.

La pena è più severa se il fatto è commesso con violenza alla persona o con minaccia o se è commesso abusando della qualità di operatore del sistema.

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano

poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

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

Tale reato si realizza quando un soggetto “*commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità*”.

La sanzione è più severa se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici. La pena è aumentata se il fatto è commesso abusando della qualità di operatore del sistema.

La pena è aumentata, altresì, nel caso il fatto sia commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

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

Questo reato si realizza quando un soggetto “*mediante le condotte di cui all'art. 635 bis (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento*”.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635 bis.

Il reato è integrato in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus).

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

Questo reato si configura quando “*il fatto di cui all’art. 635 quater (Danneggiamento di sistemi informatici o telematici) è diretto a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento*”.

La sanzione è più severa se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile nonché nelle ipotesi in cui il fatto sia stato commesso con abuso della qualità di operatore del sistema.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635 ter), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un Dipendente cancelli file o dati, relativi ad un’area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l’amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

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*”.

Questo reato può essere commesso da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata. La Società, tuttavia, non effettua attività di certificazione di firma elettronica.

Protezione del diritto d’autore e di altri diritti connessi al suo esercizio (art. 171 comma 1 lett. a) bis e comma 3 legge n. 633/1941 “L.a.”)

In relazione alla fattispecie delittuosa di cui all’art. 171, il Decreto ha preso in considerazione

esclusivamente due fattispecie, ovvero:

- a) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa;
- b) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Se dunque nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 bis L.a.)

La norma in esame è volta a tutelare il corretto utilizzo dei software e delle banche dati.

Per ciò che concerne i software, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".

Il reato in ipotesi si configura nel caso in cui taluno abusivamente duplichi, per trarne profitto, programmi per elaboratore o ai medesimi fini importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale o conceda in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.

Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Il secondo comma della stessa norma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduca, trasferisca su altro supporto, distribuisca, comunichi, presenti o dimostri in pubblico il contenuto di una banca dati ovvero esegua l'estrazione o il reimpiego della banca dati in violazione delle disposizioni di cui alla Legge sul Diritto d'Autore.

Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicché assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 ter L.a.)

La disposizione in esame tende alla tutela di una serie numerosa di opere dell'ingegno: opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche.

A restringere l'ambito di applicabilità della disposizione, però, vi sono due requisiti.

Il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, necessario per integrare il fatto tipico.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 septies L.a.)

La disposizione in esame è posta a tutela delle funzioni di controllo della SIAE, in un'ottica di tutela anticipata del diritto d'autore. Si tratta pertanto di un reato di ostacolo che si consuma con la mera violazione dell'obbligo.

La disposizione estende la pena prevista dal primo comma dell'art. 173 bis ai produttori e agli importatori dei supporti non soggetti al contrassegno SIAE che non comunichino alla SIAE stessa entro trenta giorni dall'importazione o dalla commercializzazione i dati necessari all'univoca identificazione dei supporti medesimi.

Il secondo comma punisce invece la falsa comunicazione di tali dati alla SIAE.

Come in altri settori, quindi, si è voluta accordare una tutela penale alle funzioni di vigilanza delle Autorità preposte al controllo.

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 octies L.a.)

La disposizione punisce chi, a fini fraudolenti, produce, pone in vendita, promuove, installa, modifica, utilizza per uso pubblico o privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

L'art. definisce inoltre ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti

italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

Vale a restringere l'ambito di applicabilità della norma l'elemento soggettivo di perseguimento di fini fraudolenti.

CAPITOLO G.2

A seguito di una approfondita analisi della realtà aziendale, le principali Attività Sensibili che la Società ha individuato al proprio interno sono le seguenti:

1. gestione del sistema informatico;
2. utilizzo di software e di banche dati;
3. attività di comunicazione (pubblicizzazione tramite sito internet, stampa, ecc.).

CAPITOLO G.3

G.3.1 Regole e principi generali

Obiettivo della presente Parte Speciale è che tutti i Destinatari del Modello si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei Reati Informatici e dei Delitti commessi in violazione del diritto d'autore.

In particolare, non è ammesso:

- divulgare informazioni relative ai sistemi informatici aziendali;
- utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta;
- utilizzare in maniera impropria contenuti coperti dal diritto d'autore altrui;
- utilizzare segreti aziendali altrui.

Al fine di mitigare il rischio di commissione dei delitti *de quibus* e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, assolve i seguenti adempimenti:

1. fornisce, ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli *username* e delle *password* per accedere ai principali sistemi informatici utilizzati;
2. limita, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
3. effettua, per quanto possibile, nel rispetto della normativa sulla privacy e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
4. predispone e mantiene adeguate difese a protezione dei server della Società;
5. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

CAPITOLO G.4

G.4.1 Principi comportamentali specifici

Ai fini dell'attuazione delle regole e del rispetto dei divieti elencati al precedente paragrafo, devono essere rispettati i principi comportamentali qui di seguito descritti.

In particolare:

1. è vietato introdurre in azienda e collegare al sistema informatico aziendale computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato;
2. è vietato modificare la configurazione di postazioni di lavoro fisse o mobili;
3. è vietato acquisire, possedere o utilizzare strumenti *software* e/o *hardware* che potrebbero essere adoperati per 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, ecc.);
4. 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;
5. è vietato divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
6. è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
7. è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
8. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
9. è vietato 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;
10. è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, 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;
11. 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;

12. 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.

La Società si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1. 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;
2. 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;
3. diffidare i Dipendenti dall'utilizzare il PC aziendale per uso personale;
4. informare i Dipendenti e gli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
5. impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
6. 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;
7. limitare gli accessi alla stanza server unicamente al personale autorizzato;
8. 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;
9. fornire ogni sistema informatico di adeguato software *firewall* e *antivirus* e far sì, ove possibile, che questi non possano venir disattivati;
10. impedire l'installazione e l'utilizzo di software non approvati dalla Società e non correlati con l'attività professionale espletata per la stessa;
11. limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (cosiddetti "*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);
12. impedire l'installazione e l'utilizzo, sui sistemi informatici della Società, di software (cosiddetti "P2P", di *files sharing* o di *istant 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 e sensibilizzare il personale ad adottare i programmi della Società che forniscono i medesimi servizi;
 13. 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 alla Società, possano illecitamente collegarsi alla rete Internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai Dipendenti;
 14. 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;
 15. informare tempestivamente i responsabili del sistema informatico dell'avvio e della cessazione di rapporti di lavoro del personale dipendente e dei collaboratori al fine di attivare il processo di rilascio, modifica e revoca delle abilitazioni;
 16. prevedere l'obbligo di segnalazione delle irregolarità riscontrate nell'utilizzo delle abilitazioni;
 17. 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;
 18. effettuare periodicamente controlli al fine di verificare che non vi sia l'utilizzo di un numero di licenze superiori rispetto a quelle concordate con i fornitori dei relativi *software*;
 19. tenere un registro di tutti i *software* in uso per lo svolgimento delle attività della Società, scadenzando i termini delle relative licenze;
 20. prevedere nei contratti con i fornitori dei *software* informatici una clausola di manleva a favore della Società in caso di violazione di diritti di soggetti terzi;

21. effettuare controlli periodici sui *software* installati nei terminali aziendali al fine di individuare eventuali installazioni di programmi non autorizzati, prevedendo anche l'eliminazione forzata di eventuali contenuti non autorizzati;
22. verificare periodicamente la corrispondenza tra le banche dati in uso e il numero delle licenze ottenute per il relativo utilizzo;
23. effettuare un controllo sistematico e formalizzato sulla fonte di provenienza delle immagini utilizzate per presentazioni e brochure pubblicitarie;
24. verificare che i video e la musica eventualmente diffusi tramite la rete Internet e intranet avvenga nel rispetto di diritti di proprietà intellettuale eventualmente spettanti a terzi;
25. verificare periodicamente che sul sito internet aziendale non venga pubblicato materiale non autorizzato;
26. informare i Destinatari dell'importanza di un corretto utilizzo del materiale protetto dal diritto d'autore altrui e, in particolare, sulle corrette modalità di selezione e utilizzo delle immagini in occasione della realizzazione di materiale pubblicitario;
27. prevedere, in tutti i contratti stipulati con le società di comunicazione o con le agenzie pubblicitarie, l'obbligo a carico delle stesse di procurarsi tutte le licenze necessarie all'utilizzo delle opere artistiche inserite nelle campagne promozionali (tra cui, ad esempio, video, immagini e contenuti musicali, ecc.).

CAPITOLO G. 5

CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella policy aziendale adottata ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

CAPITOLO G.6

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, sono previsti i seguenti flussi informativi nei confronti dell'Organismo di Vigilanza:

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Amministratore di Sistema	Descrizione di criticità evidenziate sui sistemi informatici (ad esempio accesso forzato a sistemi protetti o non autorizzato a stanze server, manomissione di dati ecc.). Eventuali criticità rilevate sull'utilizzo delle licenze software.	Ad evento

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

PARTE SPECIALE – H – REATI TRIBUTARI

CAPITOLO H. 1

H.1.1. Le fattispecie dei reati tributari (art. 25-*quinquiesdecies*, D. Lgs. n. 231/2001)

Il Decreto Legge 26 ottobre 2019, n. 124 recante “*Disposizioni urgenti in materia fiscale e per esigenze indifferibili*”, convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 (entrata in vigore il 25 dicembre 2019) ha introdotto nel D.Lgs. n. 231/2001 l’art. 25-*quinquiesdecies* (“*Reati tributari*”).

L’art. 25-*quinquiesdecies* del D. Lgs. 231/2001 è poi stato integrato dal D.Lgs. 14 luglio 2020, n. 75 (di attuazione della cosiddetta “Direttiva PIF”). In particolare, tale ultimo decreto, entrato in vigore in data 30 luglio 2020, ha aggiunto all’art. 25-*quinquiesdecies* un nuovo comma 1-*bis*, ai sensi del quale acquisiscono rilevanza, ai fini della responsabilità amministrativa degli enti, ulteriori reati fiscali, laddove siano

- “*commessi nell’ambito di sistemi fraudolenti transfrontalieri e*
- *al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*”.

Al fine di assicurare una corretta comprensione della presente Parte Speciale da parte di tutti i Destinatari del presente Modello, vengono di seguito descritte le fattispecie previste dal D. Lgs. 10 marzo 2000, n. 74 espressamente richiamate all’interno dell’art. 25-*quinquiesdecies*.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 d.lgs. 74/2000)

Il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell’amministrazione finanziaria.

È prevista una pena inferiore se l’ammontare degli elementi passivi fittizi è inferiore a Euro centomila.

Dichiarazione fraudolenta mediante altri artifici (art. 3 d.lgs. 74/2000)

Fuori dai casi previsti dall’articolo precedente, il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l’accertamento e ad indurre in errore l’amministrazione

finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a Euro trentamila; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a Euro unmilione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a Euro trentamila.

Anche per tale fattispecie, è previsto che il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 d.lgs. 74/2000)

Il reato in oggetto è commesso da chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Al comma 2, viene precisato che l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

È prevista una pena inferiore se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a Euro centomila.

Occultamento o distruzione di documenti contabili (art. 10 d.lgs. 74/2000)

Il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Sottrazione fraudolenta al pagamento di imposte (art. 11 d.lgs. 74/2000)

La fattispecie prevista al primo comma dell'articolo in oggetto è commessa da chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi

o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad Euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

È prevista una pena più severa se l'ammontare delle imposte, sanzioni ed interessi è superiore a Euro duecentomila.

La fattispecie prevista al secondo comma è commessa da chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad Euro cinquantamila.

È prevista una pena più severa se l'ammontare delle imposte, sanzioni ed interessi è superiore a Euro duecentomila.

Dichiarazione infedele (art. 4 d.lgs. 74/2000)

Fuori dei casi previsti dagli articoli 2 e 3, tale reato è configurabile a carico di chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

Fuori dei casi di cui al precedente, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).

Tale reato assume rilevanza ai sensi del Decreto 231 se commesso nell'ambito di sistemi fraudolenti transfrontalieri, connessi al territorio di almeno un altro Stato membro

dell'Unione europea, e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

Omessa dichiarazione (art. 5 d.lgs. 74/2000)

Il reato in oggetto è commesso da chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

È punito chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Ai fini della disposizione prevista dai commi precedenti non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

Tale reato assume rilevanza ai sensi del Decreto 231 se commesso nell'ambito di sistemi fraudolenti transfrontalieri, connessi al territorio di almeno un altro Stato membro dell'Unione europea, e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

Indebita compensazione (art. 10-quater d.lgs. 74/2000)

Il reato in oggetto è commesso da chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.

Il reato è integrato altresì da chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

Tale reato assume rilevanza ai sensi del Decreto 231 se commesso nell'ambito di sistemi fraudolenti transfrontalieri, connessi al territorio di almeno un altro Stato membro dell'Unione europea, e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

CAPITOLO H.2

Attività Sensibili nell'ambito dei reati tributari

In relazione ai reati trattati nella presente Parte Speciale, vengono di seguito indicate le Attività Sensibili che, per il loro contenuto intrinseco, sono considerate maggiormente esposte al rischio di commissione degli stessi.

1. Predisposizione delle dichiarazioni e gestione degli adempimenti fiscali (la fiscalità aziendale)
2. Conservazione delle scritture contabili e fiscali
3. Attività di investimento e operazioni straordinarie.

CAPITLO H.3

Principi generali di comportamento

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati nella stessa considerati, è che tutti i Destinatari del Modello si attengano al rispetto di tutti i principi che siano direttamente o indirettamente funzionali alla prevenzione di condotte idonee a integrare i reati tributari sopra richiamati.

I Destinatari dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dalla presente Parte Speciale;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure, nello svolgimento di tutte le attività finalizzate, da un lato, alla gestione della contabilità, della fatturazione, della redazione del bilancio e conservazione delle scritture contabili rilevanti ai fini fiscali e, dall'altro lato, alla gestione della fiscalità (compresa la predisposizione delle dichiarazioni fiscali e gestione degli adempimenti connessi);
4. tenere un comportamento con l'Amministrazione finanziaria (anche in caso di accertamenti, verifiche o contenziosi) improntato ai principi di correttezza, trasparenza, buona fede e professionalità;
5. rispettare gli adempimenti previsti dalla normativa fiscale.

CAPITOLO H.4

Principi procedurali specifici

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 qui di seguito descritti.

1) Predisposizione delle dichiarazioni e gestione degli adempimenti fiscali (la fiscalità aziendale)

Nella predisposizione delle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto, la Società garantisce l'implementazione e il rispetto dei seguenti presidi:

- segregazione dei ruoli tra i soggetti che predispongono le dichiarazioni fiscali e i soggetti deputati ai relativi controlli;
- segregazione dei ruoli nella gestione e conservazione della documentazione contabile rilevante ai fini fiscali;
- controllo da parte della società di revisione e del collegio sindacale (ove esistente);
- adeguato tracciamento di tutti i flussi informativi intercorrenti tra la Società e i consulenti fiscali;
- veridicità dell'ammontare degli elementi attivi i quali non dovranno mai essere indicati per un ammontare inferiore a quello effettivo, così come non dovranno mai essere indicati elementi passivi fittizi;
- veridicità dell'ammontare di una base imponibile affinché non sia mai calcolata in misura inferiore a quella effettiva (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e/o avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
- divieto di compensare crediti inesistenti e non spettanti;
- rispetto dei termini di legge nelle dichiarazioni fiscali e negli altri adempimenti in qualità di sostituto di imposta.

La Società si impegna a garantire la massima collaborazione e trasparenza nell'ambito dei rapporti con l'Amministrazione fiscale. In particolare, la Società si impegna a garantire che:

- siano individuati espressamente i soggetti autorizzati a trasmettere comunicazioni nei confronti dell'Agenzia delle Entrate e a riscontrarne le richieste;

- qualsivoglia comunicazione di informazioni/dati/notizie nei confronti dell'Agenzia delle Entrate sia effettuata in maniera corretta ed esaustiva nell'interesse o per conto della Società, sensibilizzando su questo anche i consulenti fiscali.

2. Conservazione delle scritture contabili e fiscali

Nella predisposizione e successiva tenuta delle scritture contabili rilevanti ai fini tributari, la Società pone in essere una serie di misure formalizzate idonee ad assicurare che tutti i Dipendenti, nell'ambito delle rispettive competenze:

- rispettino il divieto di (i) emettere o utilizzare fatture o altri documenti contabili relativi ad operazioni inesistenti, (ii) emettere o utilizzare fatture o altri documenti contabili per corrispettivi superiori agli importi reali, (iii) emettere o utilizzare fatture o altri documenti contabili che indichino soggetti diversi da quelli tra cui è effettivamente intercorso il rapporto sotteso (iv) effettuare pagamenti a fronte dell'emissione di fatture relative ad attività mai ricevute;
- custodiscano in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento.

La Società si impegna, altresì, a garantire – anche tramite appositi sistemi informatici – l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione dei dati nelle dichiarazioni tributarie, con riferimento, a titolo esemplificativo, a:

- la tracciabilità dei flussi e l'identificazione dei soggetti che alimentano la trasmissione dei dati contabili e finanziari necessari alla predisposizione delle scritture contabili;
- il rispetto del principio di segregazione dei compiti e il coinvolgimento di soggetti differenti nello svolgimento delle principali attività previste (fatturazione, pagamento, archiviazione della documentazione);
- controllo sull'effettività delle prestazioni rispetto alle fatture emesse;
- verifica della veridicità delle dichiarazioni rispetto alle scritture contabili.

3. Processi di contabilità e fatturazione

Nei processi relativi alla gestione della contabilità e fatturazione, la Società garantisce i seguenti presidi:

- la tracciabilità dei flussi e l'identificazione dei soggetti che alimentano la trasmissione dei dati contabili e finanziari necessari alla predisposizione delle scritture contabili;
- in caso di operazioni su asset o altre attività (ad esempio, alienazioni di beni propri o altrui) venga effettuata una valutazione dell'identità delle controparti (interesse all'operazione, legami con soci e amministratori);
- nella gestione dei rapporti contrattuali il rispetto del principio di segregazione dei compiti e il coinvolgimento di soggetti differenti nello svolgimento delle principali attività previste (fatturazione, pagamento, archiviazione della documentazione);
- il rispetto del divieto di (i) emettere o utilizzare fatture o altri documenti contabili relativi ad operazioni inesistenti, (ii) emettere o utilizzare fatture o altri documenti contabili per corrispettivi superiori agli importi reali, (iii) emettere o utilizzare fatture o altri documenti contabili che indichino soggetti diversi da quelli tra cui è effettivamente intercorso il rapporto sotteso (iv) effettuare pagamenti a fronte dell'emissione di fatture relative ad attività mai ricevute.

A completamento dei presidi previsti nella presente Parte Speciale, si fa rinvio, altresì, ai presidi previsti nella Parte Speciale C per la prevenzione del reato di Autoriciclaggio.

CAPITOLO H.5

I controlli dell'OdV

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi contenuti nelle *policy* aziendali adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

L'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verificano violazioni ai principi procedurali specifici contenuti nella presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.

È, altresì, attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti aziendali rilevanti per lo svolgimento dei propri compiti.

CAPITOLO H.6

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, sono previsti i seguenti flussi informativi nei confronti dell'Organismo di Vigilanza:

Funzione	Oggetto	Periodicità
CFO	Controlli effettuati sui processi di fatturazione nel periodo di riferimento e segnalazione di eventuali criticità rilevate. Controlli effettuati sulla tenuta della contabilità.	Annuale
	Informativa (con allegata documentazione di supporto) in merito ad eventuali comunicazioni ricevute dall'amministrazione finanziaria in merito ad attività di verifica da parte di questa (ad esempio, Questionari dell'Agenzia delle Entrate).	Ad evento

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.

PARTE SPECIALE – I – DELITTI CONTRO IL PATRIMONIO CULTURALE E
REATI DI RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E
SACHEGGIO DI BENI CULTURALI E PAESAGGISTICI

CAPITOLO I.1

I.1.1. Le fattispecie dei Delitti contro il patrimonio culturale e reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (artt. 25-*septiesdecies* e 25-*duodevicies*, D. Lgs. n. 231/2001)

La Legge 9 marzo 2022, n. 22, recante “*Disposizioni in materia di reati contro il patrimonio culturale*”, ha introdotto nel D. Lgs. n. 231/2001 gli articoli 25-*septiesdecies* (“*Delitti contro il patrimonio culturale*”) e 25-*duodevicies* (“*Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici*”).

Le fattispecie previste dai suddetti articoli puniscono una pluralità di condotte perpetrate a danno di beni culturali o paesaggistici, tutelati dal D. Lgs. 22 gennaio 2004, n. 42 (il “**Codice dei beni culturali e del paesaggio**”).

Nel concetto di “beni culturali” rientrano i beni culturali mobili e immobili, ovverosia, cose di interesse artistico, quali opere d’arte, di interesse storico, archeologico, etnoantropologico, bibliografico, documentale o archivistico o altre cose di interesse culturale oggetto di specifiche disposizioni di tutela ai sensi del Codice dei beni culturali e del paesaggio.

Nel concetto di “beni paesaggistici” rientrano gli immobili e le aree che costituiscono espressione dei valori storici, culturali, naturali, morfologici ed estetici del territorio, e in particolare gli immobili e le aree di notevole interesse pubblico, le aree tutelate per legge ed infine gli immobili e le aree comunque sottoposte alla tutela dei piani paesaggistici.

In generale, qualsiasi intervento su beni culturali o paesaggistici deve avvenire nel rispetto delle disposizioni previste dal Codice dei beni culturali e del paesaggio (ad esempio, la richiesta di specifiche autorizzazioni alle Autorità competenti).

Al fine di assicurare una corretta comprensione della presente Parte Speciale da parte di tutti i Destinatari del presente Modello, vengono di seguito descritte le fattispecie espressamente richiamate all’interno degli artt. 25-*septiesdecies* e 25-*duodevicies* del Decreto, che appaiono potenzialmente rilevanti in relazione all’operatività della Società.

Furto di beni culturali (art. 518 c.p.)

Il reato punisce la condotta di chiunque si impossessa di un bene culturale mobile altrui, sottraendolo a chi lo detiene, al fine di trarne profitto, per sé o per altri, o si impossessa di beni culturali appartenenti allo Stato, in quanto rinvenuti nel sottosuolo o nei fondali marini.

Appropriazione indebita di beni culturali (art. 518-ter c.p.)

La norma in oggetto punisce chiunque, al fine di procurare a sé o ad altri un ingiusto profitto, si appropria di un bene culturale altrui di cui abbia, a qualsiasi titolo, il possesso.

Ricettazione di beni culturali (art. 518-quater c.p.)

Il reato in oggetto è integrato dalla condotta di chi, fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta beni culturali provenienti da un qualsiasi delitto, o comunque si intromette nel farli acquistare, ricevere od occultare.

Riciclaggio di beni culturali (art. 518-sexies c.p.)

Il reato in oggetto punisce, fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce beni culturali provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.)

La norma punisce chiunque forma, in tutto o in parte, una scrittura privata falsa o, in tutto o in parte, altera, distrugge, sopprime od occulta una scrittura privata vera, in relazione a beni culturali mobili, al fine di farne apparire lecita la provenienza.

Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.)

La norma in esame punisce: (i) chiunque senza la prescritta autorizzazione, aliena o immette sul mercato beni culturali; (ii) chiunque essendovi tenuto, non presenta, nel termine di trenta giorni, la denuncia degli atti di trasferimento della proprietà o della detenzione di beni culturali; (iii) l'alienante di un bene culturale soggetto a prelazione che effettua la consegna della cosa in pendenza del termine di sessanta giorni dalla data di ricezione della denuncia di trasferimento.

Uscita o esportazione illecite di beni culturali (art. 518-undecies)

Il reato in oggetto è integrato dalla condotta di chiunque trasferisce all'estero beni culturali, cose di interesse artistico, storico, archeologico, etnoantropologico, bibliografico,

documentale o archivistico o altre cose oggetto di specifiche disposizioni di tutela ai sensi della normativa sui beni culturali, senza attestato di libera circolazione o licenza di esportazione.

Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.)

La norma in esame punisce chiunque:

- 1) distrugge, disperde, deteriora o rende in tutto o in parte inservibili o non fruibili beni culturali o paesaggistici propri o altrui;
- 2) fuori dei casi di cui al punto 1), deturpa o imbratta beni culturali o paesaggistici propri o altrui, ovvero destina beni culturali a un uso incompatibile con il loro carattere storico o artistico ovvero pregiudizievole per la loro conservazione o integrità.

Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.)

Il reato in oggetto punisce chiunque, fuori dei casi previsti dall'articolo 285, commette fatti di devastazione o di saccheggio aventi ad oggetto beni culturali o paesaggistici ovvero istituti e luoghi della cultura.

CAPITOLO I.2

Attività Sensibili nell'ambito dei Delitti contro il patrimonio culturale e reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici

In relazione ai reati trattati nella presente Parte Speciale, vengono di seguito indicate le Attività Sensibili che, per il loro contenuto intrinseco, sono considerate maggiormente esposte al rischio di commissione degli stessi.

1. Gestione – mediante affidamento in appalto – delle attività relative a:
 - (i) scavo e movimentazione terra per l'installazione di pali dell'illuminazione pubblica e installazione di corpi illuminanti nei pressi di edifici e strade di interesse storico e culturale.

CAPITOLO I.3

Principi generali di comportamento

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati nella stessa considerati, è che tutti i Destinatari del Modello si attengano al rispetto di tutti i principi che siano direttamente o indirettamente funzionali alla prevenzione di condotte idonee a integrare i Reati sopra richiamati.

I Destinatari dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dalla presente Parte Speciale;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Ai Destinatari è fatto divieto di:

- appropriarsi di beni culturali altrui;
- ricevere, occultare o, comunque, intromettersi nel fare acquistare ricevere od occultare beni culturali, oppure sostituirli, trasferirli o compiere in relazione ad essi operazioni in modo da ostacolarne la provenienza;
- formare (in tutto o in parte) o alterare scritture private in relazione a beni culturali mobili;
- alienare o immettere sul mercato, senza la prescritta autorizzazione, beni culturali;
- trasferire all'estero beni culturali, cose di interesse artistico, storico, archeologico, etnoantropologico, bibliografico, documentale o archivistico o altre cose oggetto di specifiche disposizioni di tutela ai sensi del Codice dei beni culturali e del paesaggio, senza attestato di libera circolazione o licenza di esportazione;
- commettere fatti di devastazione o di saccheggio aventi ad oggetto beni culturali o paesaggistici ovvero istituti e luoghi della cultura.

CAPITOLO I.4

Principi procedurali specifici

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 qui di seguito descritti.

In particolare, la Società garantisce che

- prima di procedere alla realizzazione di interventi presso edifici di interesse storico e artistico siano richieste le necessarie autorizzazioni/nulla osta e siano effettuate le necessarie segnalazioni/comunicazioni all'Autorità competente (i.e. la Soprintendenza competente per territorio);
- in caso di ritrovamento nelle attività di scavo di reperti di presumibile interesse archeologico, storico e artistico, siano richieste le necessarie autorizzazioni/nulla osta e siano effettuate le necessarie segnalazioni/comunicazioni all'Autorità competente (i.e. la Soprintendenza competente per territorio);
- ove richiesto/necessario, sia incaricato un esperto archeologo, cui sia demandato il compito di supervisionare e verificare – per quanto di competenza – lo svolgimento dei lavori e di comunicare gli interventi effettuati all'Autorità competente;
- in caso di nomina di esperti archeologi o altri consulenti, siano rispettate le regole di selezione e contrattualizzazione previste per i consulenti e fornitori dal Modello 231 della Società;
- qualora nella preparazione del cantiere e durante i lavori si evidenziassero ritrovamenti di presumibile interesse archeologico, storico e artistico, siano immediatamente sospesi i lavori, avendo cura di lasciare intatti i ritrovamenti, e siano effettuate le necessarie segnalazioni/comunicazioni all'Autorità competente;
- siano coinvolti più soggetti (interni o esterni) nella gestione delle tematiche sopra esposte;

- l’effettuazione dei lavori sia svolta nel rispetto delle prescrizioni rilasciate dalle Autorità competenti a tutela del paesaggio e del patrimonio culturale;
- sia svolto il monitoraggio dell’attività effettuata da soggetti terzi (appaltatori, subappaltatori) presso i cantieri, al fine di garantire il rispetto della normativa dettata dal Codice dei beni culturali e del paesaggio nonché dai Regolamenti degli enti locali di volta in volta applicabili e delle prescrizioni rilasciate dalle Autorità competenti;
- la Società garantisca che i contratti con appaltatori e subappaltatori contengano clausole che contemplino il rispetto, da parte di detti soggetti, della normativa dettata dal Codice dei beni culturali e del paesaggio.

A completamento dei presidi previsti nella presente Parte Speciale, con riferimento alla gestione dei rapporti con le Autorità competenti (i.e. la Soprintendenza), si fa rinvio, altresì, ai presidi previsti nella Parte Speciale A per la gestione dei rapporti con la Pubblica Amministrazione.

CAPITOLO I.5

I controlli dell'OdV

L'OdV 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.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi contenuti nelle *policy* aziendali adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

L'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verificano violazioni ai principi procedurali specifici contenuti nella presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.

È, altresì, attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti aziendali rilevanti per lo svolgimento dei propri compiti.

CAPITOLO I.6

FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, sono previsti i seguenti flussi informativi nei confronti dell'Organismo di Vigilanza:

Funzione	Oggetto	Periodicità
Amministratore Unico	Informativa in merito al ritrovamento, presso i cantieri della Società, di beni di interesse storico, artistico, archeologico o comunque soggetti alla normativa del Codice dei beni culturali e del paesaggio.	Ad evento
	Informativa in merito a eventuali violazioni della normativa del Codice dei beni culturali e del paesaggio commesse da appaltatori e subappaltatori, presenti presso i cantieri della Società.	Ad evento
Amministratore Unico	Informativa in merito all'eventuale acquisizione di immobili soggetti a vincoli culturali e/o paesaggistici.	Ad evento

Le funzioni aziendali sopra indicate sono sia interne a Lumagest sia fornite in *outsourcing* da City Green Light.